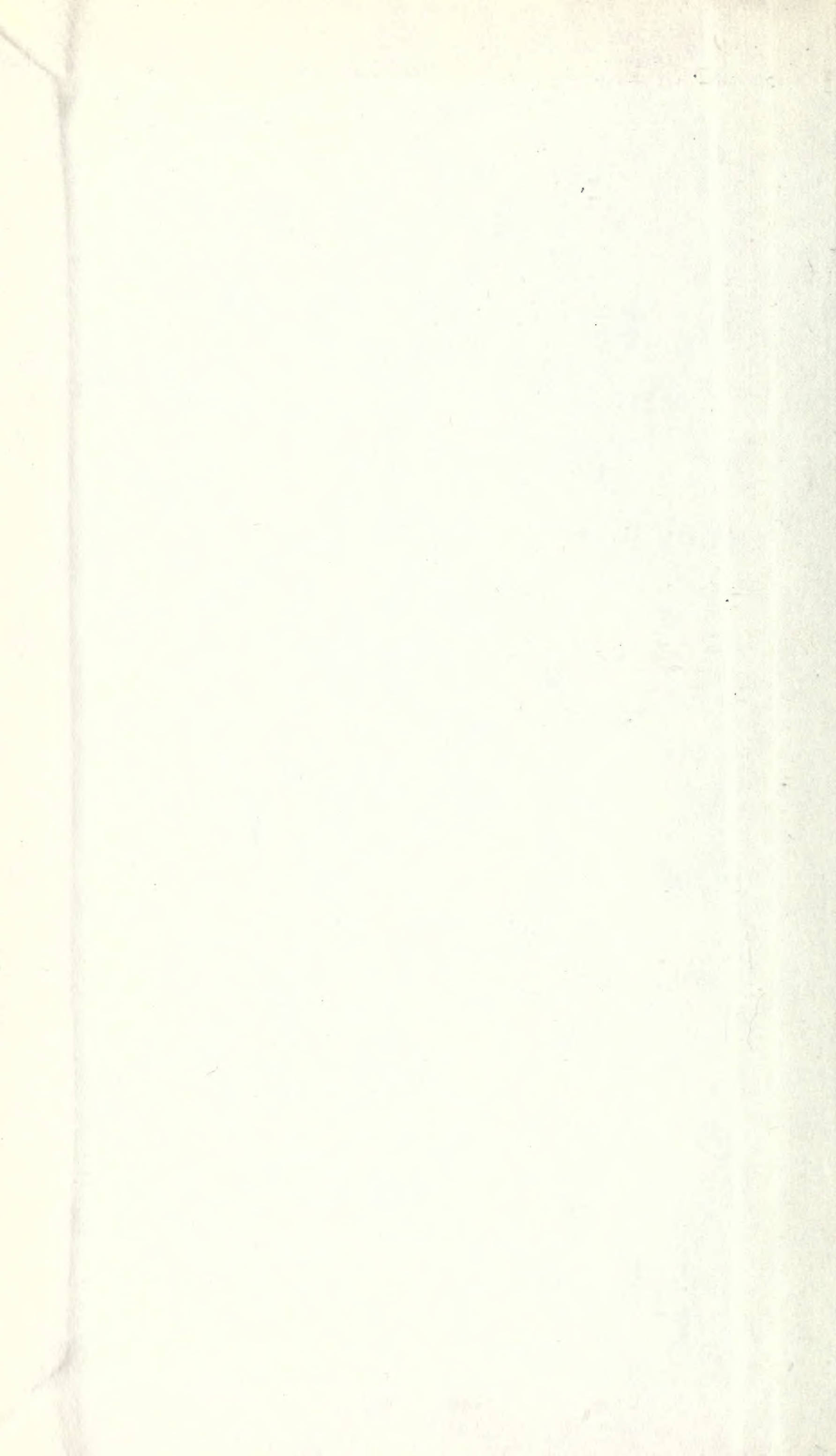
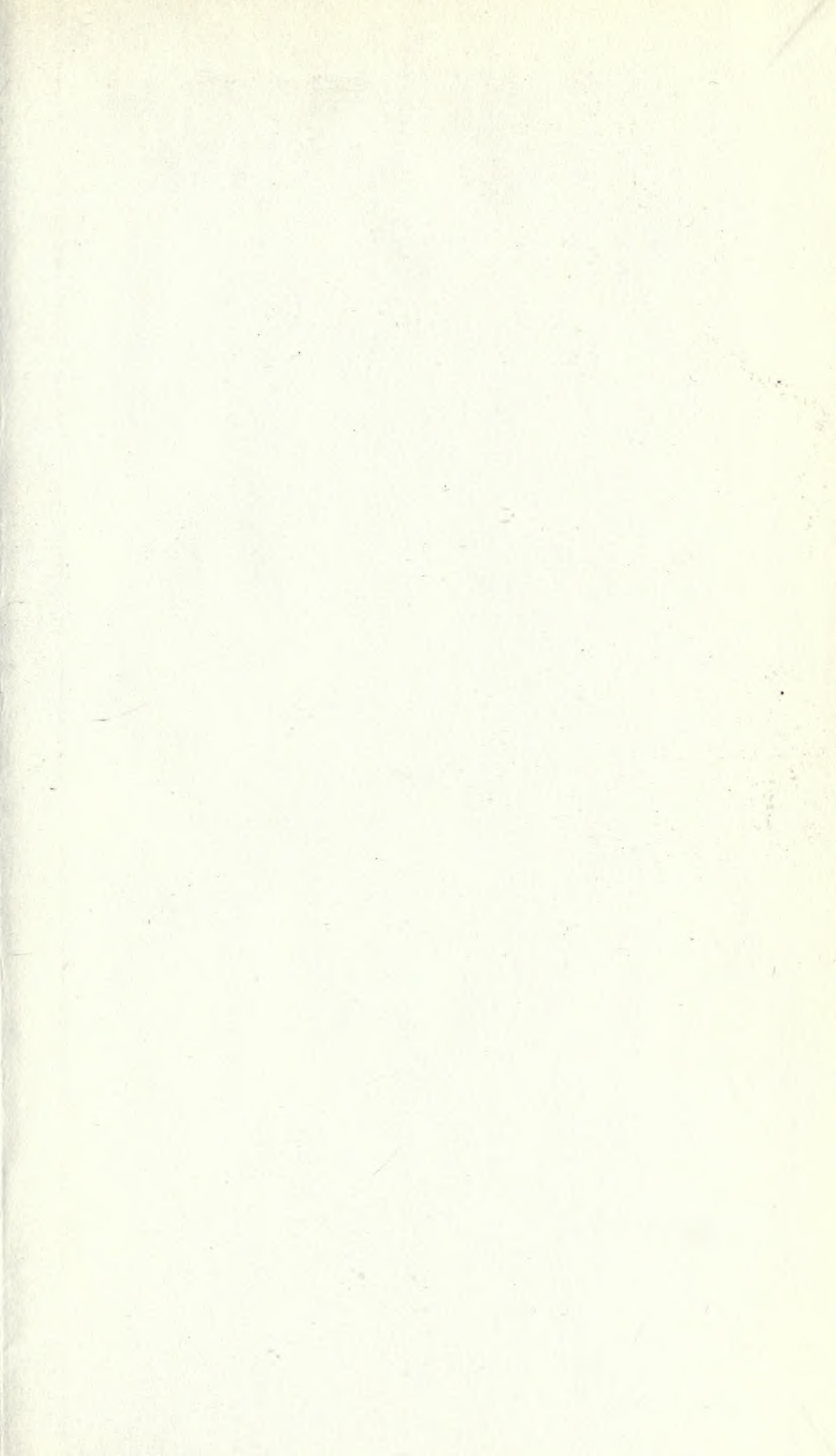
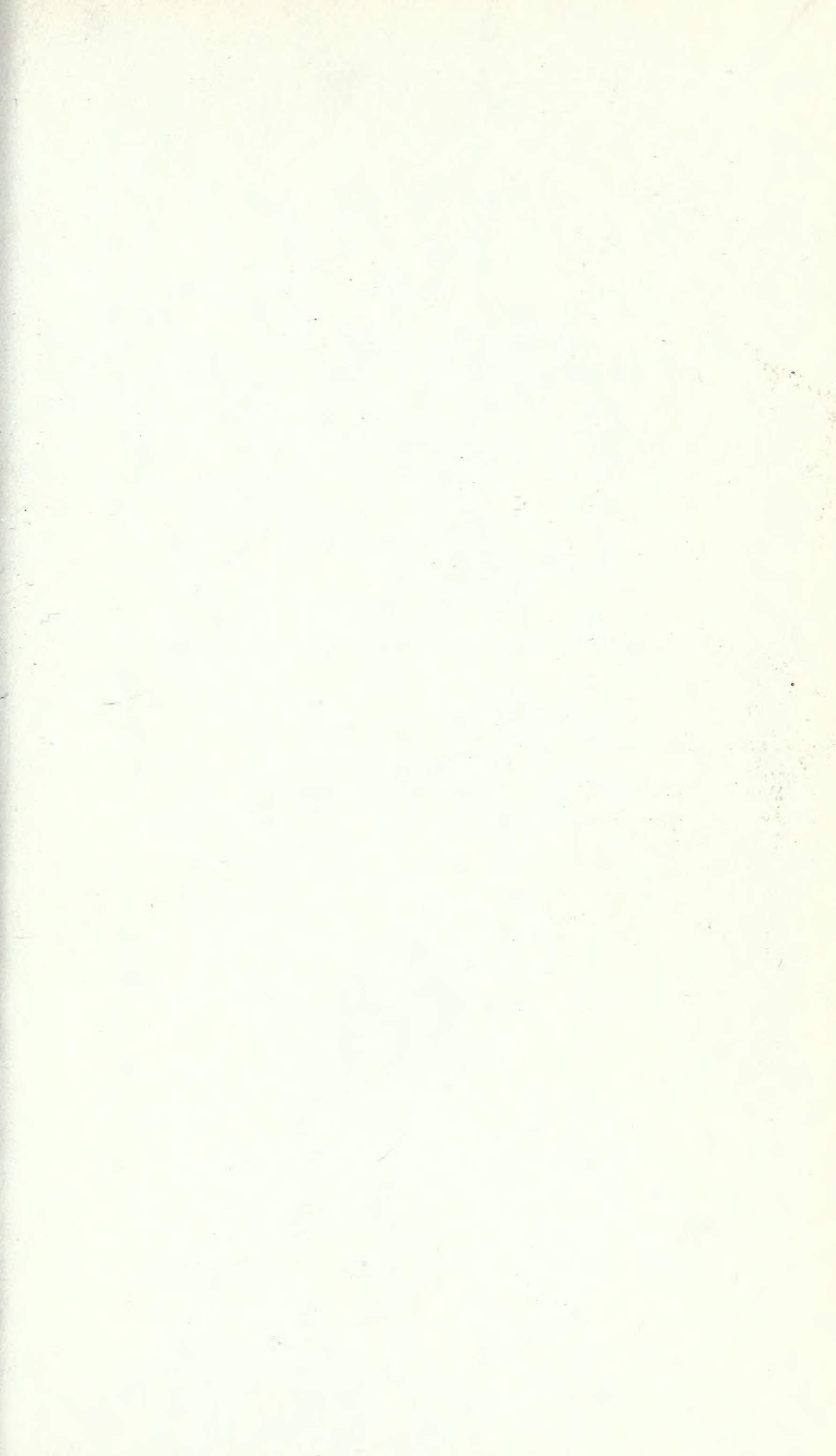

UNIVERSITY OF TORONTO
3 1761 00479360 0













HANDBUCH

DER

HÖHEREN ALGEBRA

VON

J. A. SERRET.

DEUTSCH BEARBEITET VON G. WERTHEIM.

ZWEITER BAND.



LEIPZIG,
DRUCK UND VERLAG VON B. G. TEUBNER.
1868.


DUBLETTE

Inhaltsverzeichniss.

Drittes Kapitel.

Eigenschaften der ganzen Functionen einer Veränderlichen in Beziehung auf einen Primzahlmodul.

Viertes Kapitel.

Ueber die Anzahl der zwischen gegebenen Grenzen enthaltenen Primzahlen.

Vierter Theil.

Die Substitutionen.

Erstes Kapitel.

Allgemeine Eigenschaften der Substitutionen.

Zweites Kapitel.

Eigenschaften der Systeme conjugirter Substitutionen.

Drittes Kapitel.

Indices der conjugirten Systeme.

Viertes Kapitel.

Ueber einige besondere Fälle der Theorie der Substitutionen.

Fünftes Kapitel.

Anwendungen der Theorie der Substitutionen.

Fünfter Theil.

Die algebraische Auflösung der Gleichungen.

Erstes Kapitel.

Gleichungen dritten und vierten Grades. Allgemeine Betrachtungen über die algebraische Auflösung der Gleichungen.

Zweites Kapitel.

Ueber die Unmöglichkeit, allgemeine Gleichungen, deren Grad grösser als 4 ist, algebraisch aufzulösen.

Drittes Kapitel.

Abel'sche Gleichungen.

Viertes Kapitel.

Ueber eine Klasse von Gleichungen neunten Grades, die algebraisch auflösbar sind.

Fünftes Kapitel.

Ueber die algebraisch auflösbaren Gleichungen.

Die allgemeinen Eigenschaften der Gleichungen und die darauf bezüglichen analytischen Fragen sind im ersten Bande dieses Werkes behandelt; wir haben uns jetzt noch mit der algebraischen Auflösung der Gleichungen zu beschäftigen.

Ehe wir aber diese wichtige Frage, die wir hauptsächlich im Auge haben, in Angriff nehmen, müssen wir die partiellen Theorien entwickeln, die wir später zu benutzen haben. Da diese Theorien schon an sich selbst von grossem Interesse sind, so werden wir sie eingehend darlegen.



Dritter Theil.

Eigenschaften der ganzen Zahlen.



Erstes Kapitel.

Congruenzen.

Congruente oder äquivalente Zahlen.

281. Wenn die Differenz zweier positiven oder negativen ganzen Zahlen a und b durch eine dritte positive Zahl M theilbar ist, so heissen a und b in Beziehung auf M congruent oder äquivalent; der Divisor M wird der Modul genannt; jede der beiden Zahlen a und b ist der Rest der andern nach dem Modul M.

Um auszudrücken, dass a und b in Beziehung auf den Modul M congruent sind, genügt es, zu schreiben

$$a = b \pm \text{ein Multiplum von } M.$$

Wir werden uns aber der von Gauss eingeführten bequemeren Bezeichnung bedienen und schreiben

$$a \equiv b \ (mod.\ M);$$

diese Formel nennen wir eine Congruenz.

Bezeichnet r den Rest der Division von a durch M, so ist

$$a \equiv r \ (mod.\ M).$$

Da man es nun stets so einrichten kann, dass r zwischen 0 und M, oder auch zwischen $-\frac{M}{2}$ und $+\frac{M}{2}$ liegt, so hat jede Zahl einen Rest, dessen absoluter Werth nicht grösser ist, als die Hälfte des Moduls. Man nennt ihn den kleinsten Rest. Will man aber nur positive Reste betrachten, so sind die Grenzen für den kleinsten Rest 0 und M, und derselbe kann grösser sein als $\frac{M}{2}$.

282. Die Gaussische Darstellungsart der Congruenzen lässt die Analogie klar zu Tage treten, welche zwischen den Con-

gruenzen und den Gleichungen besteht, ohne gleichwohl zu irgend einem Missverständniss Veranlassung zu geben. Wir wollen jetzt zeigen, dass die meisten Transformationen, die man mit Gleichungen vornehmen kann, auch auf Congruenzen angewandt werden können.

Addition und Subtraction. — Hat man

$$a \equiv b \pmod{M},$$
$$a' \equiv b' \pmod{M},$$

so ist auch

$$a \pm a' \equiv b \pm b' \pmod{M}.$$

Die vorgelegten Congruenzen drücken nämlich aus, dass

$$a = b + \text{ein Multiplum von } M,$$
$$a' = b' + \text{ein Multiplum von } M$$

ist; folglich ist

$$a \pm a' = b \pm b' + \text{ein Multiplum von } M,$$

oder

$$a \pm a' \equiv b \pm b' \pmod{M}.$$

Multiplication. — Man kann eine Congruenz mit einer beliebigen ganzen Zahl multipliciren; denn ist

$$a \equiv b \pmod{M},$$

d. h.

$$a = b + \text{ein Multiplum von } M,$$

so hat man auch für jeden ganzen Werth von m

$$ma = mb + \text{ein Multiplum von } M,$$

oder

$$ma \equiv mb \pmod{M}.$$

Man kann ferner mehrere Congruenzen, die sich auf denselben Modul beziehen, mit einander multipliciren. Ist nämlich

$$a \equiv b \pmod{M.},$$
$$a' \equiv b' \pmod{M.},$$

oder

$$a = b + \text{ein Multiplum von } M,$$
$$a' = b' + \text{ein Multiplum von } M,$$

so ergiebt sich durch Multiplication

$$aa' = bb' + \text{ein Multiplum von } M,$$

oder

$$aa' \equiv bb' \pmod{M}.$$

Hat man allgemein

$$\left.\begin{array}{l} a \equiv b \\ a' \equiv b' \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ a^{(m)} \equiv b^{(m)} \end{array}\right\} (mod.\ M),$$

so ist auch

$$a a' \ldots a^{(m)} \equiv b b' \ldots b^{(m)} \ (mod.\ M).$$

Potenzirung. — Aus dem, was wir soeben über die Multiplication gesagt haben, folgt sofort, dass man beide Glieder einer Congruenz auf dieselbe Potenz erheben darf. Hat man also

$$a \equiv b \ (mod.\ M),$$

so ist auch

$$a^m \equiv b^m \ (mod.\ M).$$

Die Resultate, die wir bisher erlangt haben, lassen sich folgendermassen zusammenfassen:

Ist

$$f(x) = Ax^m + Bx^n + \cdots$$

eine ganze und rationale Function von x, deren Coefficienten A, B, u. s. w. ganze Zahlen sind, und hat man

$$a \equiv b \ (mod.\ M),$$

so ist auch

$$f(a) \equiv f(b) \ (mod.\ M).$$

Division. — Man darf eine Congruenz durch irgend eine ganze Zahl dividiren, welche prim zum Modul ist.

Hat man nämlich

$$m a \equiv m b \ (mod.\ M)$$

oder

$$m a = m b + M \times q,$$

so ergiebt sich, wenn durch m dividirt wird,

$$a = b + \frac{M \times q}{m}.$$

Ist nun m prim zu M, so muss q durch m theilbar sein, und man erhält

$$a = b + \text{ein Multiplum von } M,$$

oder

$$a \equiv b \ (mod.\ M).$$

Anders verhält es sich, wenn die Zahl m und der Modul M einen gemeinschaftlichen Factor haben; denn ist $\frac{M'}{m'}$ der mit $\frac{M}{m}$ gleichbedeutende irreductibele Bruch, so hat man

$$a = b + \frac{M' \times q}{m'},$$

und da diese Gleichung nur erfordert, dass q durch m' theilbar sei, so ist

$$a \equiv b \pmod{M'}.$$

Man kann eine Congruenz auch durch eine andere dividiren, wenn die Glieder der letzteren prim zum Modul sind. Dies zu beweisen, betrachten wir die Congruenzen

(1). $$aa' \equiv bb' \pmod{M},$$

(2). $$a \equiv b \pmod{M}.$$

Bezeichnet r den kleinsten Rest der Differenz $a' - b'$, so ist

(3). $$a' \equiv b' \pm r \pmod{M},$$

und durch Multiplication der Congruenzen (2) und (3) ergiebt sich

(4). $$aa' \equiv bb' \pm br \pmod{M}.$$

Aus den Congruenzen (1) und (4) folgt

$$br \equiv 0 \pmod{M}:$$

Nun ist der Voraussetzung nach M prim zu b, mithin

$$r \equiv 0 \pmod{M},$$

oder, da $r < M$ ist,

$$r = 0.$$

Man hat also

$$a' \equiv b' \pmod{M},$$ w, z. b. w.

Ueber die Zahl, welche ausdrückt, wie viele Zahlen prim zu einer gegebenen Zahl und nicht grösser als diese Zahl sind.

283. Hilfssatz. — Multiplicirt man die Terme der Reihe

(1). $$1, 2, 3, \ldots, (M-1)$$

mit einer ganzen Zahl a, die prim zu M ist, so sind die erhaltenen Producte

(2). $$a, 2a, 3a, \ldots, (M-1)a$$

in irgend einer Reihenfolge den Zahlen (1) nach dem Modul M congruent.

Keine Zahl ma der Reihe (2) kann durch M theilbar sein, da M prim zu a und grösser als m ist. Dasselbe ist der Fall mit

der Differenz $ma - m'a$ zweier Terme der Reihe (2); denn diese Differenz ist gleichfalls ein Term von (2). Bildet man also die kleinsten positiven Reste der Zahlen (2) in Beziehung auf M, so sind diese Reste sämmtlich von einander verschieden, und keiner derselben ist Null; sie stimmen daher, abgesehen von der Reihenfolge, mit den Zahlen der Reihe (1) überein.

Zusatz. — Wenn die Zahl M prim zu a ist, so sind die Terme der arithmetischen Progression

(1). $$c\,,\ c + a\,,\ c + 2a\,,\ \ldots\,,\ c + (M - 1)\,a$$

für jeden beliebigen ganzen Werth von c beziehungsweise den Zahlen

(2). $$0\,,\ 1\,,\ 2\,,\ \ldots\,,\ (M - 1)$$

nach dem Modul M congruent.

Nach dem vorhergehenden Hilfssatze sind nämlich die Zahlen (1) beziehungsweise den Zahlen

$$c\,,\ c + 1\,,\ c + 2\,,\ \ldots\,,\ c + (M - 1)\,,$$

letztere aber offenbar den Zahlen (2) nach dem Modul M congruent.

284. Wir bedienen uns des Symbols $\varphi(M)$, um auszudrücken, wie viele Zahlen es giebt, welche prim zu M und nicht grösser als M sind. Nach dieser Definition ist augenscheinlich

$$\varphi(1) = 1.$$

Lehrsatz. — Bezeichnet M das Produkt mehrerer Zahlen $a, b, \ldots, l$, von denen je zwei prim zu einander sind, so ist

$$\varphi(M) = \varphi(a)\,\varphi(b)\,\ldots\,\varphi(l).$$

Wir wollen zunächst den Fall erörtern, in welchem

$$M = ab$$

ist, wo a und b relative Primzahlen bezeichnen. Die ab ersten Zahlen können in folgender Weise geordnet werden:

$$\begin{array}{llll}
1\,, & 2\,,\ldots, & k\,,\ldots, & b, \\
b+1\,, & b+2\,,\ldots, & b+k\,,\ldots, & b+b, \\
2b+1\,, & 2b+2\,,\ldots, & 2b+k\,,\ldots, & 2b+b, \\
\ldots & \ldots & \ldots & \ldots, \\
(a-1)\,b+1\,, & (a-1)\,b+2\,,\ldots, & (a-1)\,b+k\,,\ldots, & (a-1)\,b+b.
\end{array}$$

Betrachten wir eine der Verticalreihen dieser Tabelle, z. B. die-

jenige, welche mit k beginnt. Ist k prim zu b, so ist auch jeder folgende Term dieser Reihe prim zu b; haben aber k und b einen von 1 verschiedenen gemeinschaftlichen Divisor, so giebt es in der Reihe keine Zahl, die prim zu b ist. Da nun die erste Horizontalreihe $\varphi(b)$ Zahlen enthält, welche prim zu b sind, so sind in der ganzen Tabelle $\varphi(b)$ Verticalreihen vorhanden, deren sämmtliche Terme prim zu b sind, und welche alle Zahlen dieser Art, die nicht grösser als M sind, erschöpfen. Wir nehmen jetzt an, k sei prim zu b. Die mit k beginnende Verticalreihe ist eine arithmetische Progression, deren Terme nach dem Modul a beziehungsweise den Zahlen $0, 1, 2, \ldots, (a-1)$ congruent sind. Diese letzte Reihe enthält $\varphi(a)$ Zahlen, die prim zu a sind; folglich sind auch in der betrachteten Verticalreihe $\varphi(a)$ Zahlen dieser Art vorhanden. Aus all' dem geht hervor, dass unsere Tabelle $\varphi(a) \times \varphi(b)$ Zahlen enthält, welche gleichzeitig prim zu a und zu b, d. h. prim zu dem Produkte ab sind. Man hat daher

$$\varphi(M) = \varphi(a) \cdot \varphi(b).$$

Wir gehen jetzt zu dem allgemeinen Falle über, in welchem

$$M = abc \ldots l$$

ist; $a, b, c, \ldots, l$ bezeichnen Zahlen, von denen je zwei prim zu einander sind. Man erhält der Reihe nach

$$\begin{aligned} \varphi(M) &= \varphi(a) \cdot \varphi(bc \ldots l) \\ &= \varphi(a) \cdot \varphi(b) \cdot \varphi(c \ldots l) \\ &= \varphi(a) \cdot \varphi(b) \cdot \varphi(c) \cdot \varphi(\ldots l) \\ &\quad \cdots\cdots\cdots\cdots \\ &= \varphi(a) \cdot \varphi(b) \cdot \varphi(c) \ldots \varphi(l), \end{aligned}$$

und der angegebene Satz somit ist vollständig bewiesen.

285. Der vorhergehende Satz liefert ein sehr einfaches Mittel, den Werth von $\varphi(M)$ zu bestimmen.

Ist M gleich einer Primzahl p, so sind die Zahlen, welche prim zu $M = p$ und nicht grösser als diese Zahl sind, augenscheinlich folgende:

$$1, 2, 3, \ldots, (p-1);$$

man hat daher

$$\varphi(p) = p - 1.$$

Ist M gleich einer Potenz p^ν einer Primzahl p, so enthält die Reihe der $p^{\nu-1}$ Zahlen

$$p\,,\ 2p\,,\ 3p\,,\ \ldots\,,\ p^{\nu-1}\cdot p$$

offenbar alle Zahlen, die nicht grösser als M und durch p theilbar sind; man hat daher

$$\varphi(M) = p^{\nu} - p^{\nu-1} = p^{\nu-1}(p-1),$$

oder

$$\varphi(M) = M\left(1 - \frac{1}{p}\right).$$

Wir wollen endlich den allgemeinen Fall betrachten. Es seien $p, q, r, \ldots$ die ungleichen Primfactoren von M, und es werde

$$M = p^{\nu}\, q^{\mu}\, r^{\lambda} \ldots$$

vorausgesetzt, wo $\nu, \mu, \lambda, \ldots$ ganze Exponenten bedeuten. Nach No. 284 ist

$$\varphi(M) = \varphi(p^{\nu})\,\varphi(q^{\mu})\,\varphi(r^{\lambda}) \ldots;$$

ferner hat man

$$\varphi(p^{\nu}) = p^{\nu}\left(1 - \frac{1}{p}\right),$$

$$\varphi(q^{\mu}) = q^{\mu}\left(1 - \frac{1}{q}\right),$$

$$\varphi(r^{\lambda}) = r^{\lambda}\left(1 - \frac{1}{r}\right),$$

$$\ldots\ldots\ldots\ldots,$$

also

$$\varphi(M) = p^{\nu}\, q^{\mu}\, r^{\lambda} \ldots \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\ldots.$$

oder

$$\varphi(M) = M\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\ldots.$$

Man beachte noch, dass für ein ungerades M

$$\varphi(2M) = \varphi(2)\,\varphi(M),$$

oder, weil $\varphi(2) = 1$ ist,

$$\varphi(2M) = \varphi(M)$$

ist.

286. Ehe wir zu den Congruenzen übergehen, wollen wir den folgenden Satz herleiten, der uns später von Nutzen sein wird.

Lehrsatz. — Bezeichnen $d, d', d'', \ldots$ alle Divisoren der Zahl M, die Einheit und die Zahl M selbst nicht ausgeschlossen, so hat man

$$\varphi(d) + \varphi(d') + \varphi(d'') + \ldots = M.$$

Es sei

$$M = p^\nu \; q^\mu \; r^\lambda \; \ldots,$$

wo $p, q, r, \ldots$ ungleiche Primzahlen bedeuten; dann sind die Divisoren $d, d', d'', \ldots$ nichts Anderes, als die Terme des Polynoms, welches dem folgenden Produkte gleich ist:

$$(1 + p + p^2 + \cdots + p^\nu)\,(1 + q + q^2 + \cdots + q^\mu)\,(1 + r + \cdots + r^\lambda) \cdots.$$

Irgend ein Term dieses Polynoms ist von der Form $p^\alpha \, q^\beta \, r^\gamma \ldots$; ausserdem folgt aus

$$d = p^\alpha \; q^\beta \; r^\gamma \ldots,$$

dass

$$\varphi(d) = \varphi(p^\alpha)\;\varphi(q^\beta)\;\varphi(r^\gamma)\ldots$$

ist; folglich ist die Summe aller Grössen $\varphi(d)$ gleich dem Produkt der Polynome

$$\begin{array}{l} 1 + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^\nu), \\ 1 + \varphi(q) + \varphi(q^2) + \cdots + \varphi(q^\mu), \\ 1 + \varphi(r) + \varphi(r^2) + \cdots + \varphi(r^\lambda), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

Das erste dieser Polynome hat den Werth

$$1 + (p-1)\,(1 + p + p^2 + \cdots + p^{\nu-1}) = p^\nu,$$

und da die folgenden Polynome aus demselben Grunde beziehungsweise gleich $q^\mu, r^\lambda, \ldots$ sind, so hat man

$$\varphi(d) + \varphi(d') + \varphi(d'') + \cdots = p^\nu \, q^\mu \, r^\lambda \cdots = M.$$

Ueber Congruenzen im Allgemeinen.

287. Die Zahlentheorie löst hinsichtlich der Congruenzen dieselbe Aufgabe, welche die gemeine Algebra hinsichtlich der Gleichungen behandelt. Sie stellt sich im Besonderen die Aufgabe, die Werthe von x zu ermitteln, welche einer Congruenz

$$f(x) \equiv 0 \; (mod.\ M)$$

Genüge leisten; $f(x)$ bezeichnet ein ganzes und rationales Polynom, dessen Coefficienten ganze Zahlen sind. Wird diese Congruenz durch den Werth $x = a$ befriedigt, so genügt ihr nach einer früheren Bemerkung auch der Werth $x = a + kM$, worin k eine beliebige ganze Zahl ist. Daraus folgt, dass jede Lösung eine unendliche Menge anderer Lösungen liefert, welche aber sämmtlich nach dem Modul M congruent sind. Alle in ein und

derselben Formel $a + kM$ enthaltenen Lösungen können aus einer derselben, gleichviel welcher, hergeleitet werden. Da man ausserdem über die ganze Zahl k so verfügen kann, dass $a + kM$ zwischen $-\frac{M}{2}$ und $+\frac{M}{2}$, oder zwischen 0 und M liegt, so hat man sich nur mit den zwischen diesen Grenzen enthaltenen Lösungen zu beschäftigen.

Dies vorausgesetzt, nennen wir die verschiedenen zwischen 0 und M liegenden Werthe von x, welche $f(x)$ theilbar durch M machen, Wurzeln der Congruenz

$$f(x) \equiv 0 \ (mod.\ M).$$

Eine Congruenz ist identisch, wenn alle ihre Coefficienten durch den Modul theilbar sind; sie ist offenbar unmöglich, wenn ihre Coefficienten, mit Ausnahme des von x unabhängigen Terms, durch einen Factor des Moduls theilbar sind.

Bezeichnet $F(x)$ ein ganzes und rationales Polynom, dessen Coefficienten ganze Zahlen sind, so kann man die Congruenz

$$f(x) \equiv 0 \ (mod.\ M)$$

durch die gleichbedeutende

$$f(x) + MF(x) \equiv 0 \ (mod.\ M)$$

ersetzen, und sodann über die unbestimmten Coefficienten von $F(x)$ in der Weise verfügen, dass jeder Coefficient der Congruenz kleiner als M, oder sogar, wenn man will, kleiner als $\frac{M}{2}$ wird.

Congruenzen ersten Grades.

288. Die Congruenz ersten Grades

(1). $$ax + b \equiv 0 \ (mod.\ M)$$

kann auf die Form

(2). $$ax + b = My$$

gebracht werden, und die Aufsuchung ihrer Wurzeln ist darauf zurückgeführt, die ganzzahligen Lösungen (x, y) der Gleichung (2) zu ermitteln. Sind a und M prim zu einander, so ist die Gleichung (2) immer in ganzen Zahlen lösbar, und man erhält eine erste Lösung (x_0, y_0) dadurch, dass man (No. 13) $\frac{a}{M}$ in einen Kettenbruch verwandelt. Hat man einmal eine Lösung gefunden, so sind alle übrigen durch die Formeln

$$x = x_0 + Mt \;,\; y = y_0 + at$$

gegeben, in welchen t eine unbestimmte ganze Zahl bedeutet. Ueber diese unbestimmte Grösse t kann man so verfügen, dass man einen zwischen 0 und M liegenden Werth von x erhält. Wird dieser Werth mit x_0 bezeichnet, so sind die übrigen Werthe von x immer noch durch die erste der vorhergehenden Formeln bestimmt.

Daraus geht hervor, dass die Congruenz ersten Grades (1), der Modul mag beschaffen sein, wie er will, immer nur eine Wurzel besitzt, wenn der Coefficient der Unbekannten prim zum Modul ist.

Zu demselben Schlusse gelangt man mittels des Hilfssatzes der No. 283 (Zusatz). Ertheilt man nämlich x die M Werthe

$$0 \;,\; 1 \;,\; 2 \;,\; \ldots \;,\; (M-1) \;,$$

so nimmt das erste Glied der Congruenz (1) M nach dem Modul M incongruente Werthe an; daher muss einer dieser Werthe durch M theilbar sein, und der entsprechende Werth von x ist die gesuchte Wurzel.

Bezeichnet x_0 diese Wurzel, so bedient man sich nach Gauss' Vorschlag der Schreibart

$$x_0 \equiv -\frac{b}{a} \; (mod.\ M).$$

Wenn der Coefficient a nicht prim zum Modul M ist, wenn diese beiden Zahlen etwa den grössten gemeinschaftlichen Divisor d haben, so ist die Congruenz (1) nur dann lösbar, wenn auch b den Factor d enthält. Ist dies der Fall, so geht die Congruenz in Folge der Division durch d über in

$$(3). \qquad \frac{a}{d}\, x + \frac{b}{d} \equiv 0 \left(mod.\ \frac{M}{d}\right),$$

und wir gelangen auf diese Weise wieder zu dem eben erörterten Falle. Bezeichnet x_0 die Wurzel der Congruenz (3), so sind alle Werthe von x, die ihr genügen können, in der Formel

$$x = x_0 + \frac{M}{d}\, t$$

enthalten, und man sieht, dass die vorgelegte Congruenz die d Wurzeln besitzt:

$$x_0 \,.\, x_0 + \frac{M}{d} \,,\; x_0 + \frac{2M}{d} \,,\; \ldots \,,\; x_0 + \frac{(d-1)\,M}{d} \,,$$

welche nach dem Modul M incongruent sind.

289. Wenn der Modul M eine zusammengesetzte Zahl ist, so kann die Auflösung der Congruenz

(1). $$ax + b \equiv 0 \pmod{M},$$

in welcher a als prim zu M vorausgesetzt wird, auf die Auflösung mehrerer Congruenzen zurückgeführt werden, deren jede sich auf einen Factor von M als Modul bezieht.

Es sei zunächst

$$M = M_1 \, M_2,$$

wo M_1 und M_2 ganze Zahlen bedeuten.

Die Wurzel der Congruenz (1) muss offenbar auch der Congruenz

(2). $$ax + b \equiv 0 \pmod{M_1}$$

genügen. Wird die Wurzel der letzteren mit α bezeichnet, so sind die Werthe von x, welche der vorgelegten Congruenz genügen, von der Form

$$x = \alpha + M_1 \, x_1,$$

wo x_1 eine unbestimmte Grösse ist. Durch Einsetzung dieses Werthes in (1) ergiebt sich

$$(a\alpha + b) + M_1 a x_1 \equiv 0 \pmod{M}.$$

Der Voraussetzung nach ist $a\alpha + b$ durch M_1 theilbar; setzt man

$$\frac{a\alpha + b}{M_1} = b_1,$$

so geht die letzte Congruenz, wenn man sie durch M_1 dividirt, über in

$$a x_1 + b_1 \equiv 0 \pmod{M_2}.$$

Bezeichnet α_1 die Wurzel dieser neuen Congruenz, so liefert die Formel

$$x = \alpha + M_1 \, \alpha_1$$

die Wurzel der vorgelegten Congruenz (1).

Diese Betrachtung zeigt, dass, wenn

$$M = M_1 \, M_2 \ldots M_k$$

ist, wo $M_1, M_2, \ldots, M_k$ ganze Zahlen bedeuten, die Auflösung der Congruenz

$$ax + b \equiv 0 \pmod{M}$$

zurückgeführt werden kann auf die anderer Congruenzen von der Form

$$\begin{aligned} ax + b &\equiv 0 \ (mod.\ M_1), \\ ax + b_1 &\equiv 0 \ (mod.\ M_2'), \\ &\ldots\ldots\ldots; \\ ax + b_{k-1} &\equiv 0 \ (mod.\ M_k). \end{aligned}$$

Im Besonderen kann man für die Zahlen M_1, M_2, ... die Primfactoren nehmen, deren Produkt der Modul ist.

Beispiel. — Es soll die Congruenz

$$1237\,x - 4096 \equiv 0 \ (mod.\ 675)$$

aufgelöst werden. Der Modul 675 ist gleich dem Produkte 27×25; man kann daher mit der Auflösung der Congruenz

$$1237\,x - 4096 \equiv 0 \ (mod.\ 27)$$

beginnen, welche, wenn die Coefficienten durch ihre kleinsten Reste ersetzt werden, in

$$5\,x - 8 \equiv 0 \ (mod.\ 27),$$

oder auch in

$$x = \frac{8 + 27\,y}{5}$$

übergeht. Dem Werthe $y = 1$ entspricht $x = 7$; man muss folglich

$$x = 7 + 27\,x_1$$

machen. Substituirt man diesen Werth in die vorgelegte Congruenz, so ergiebt sich

$$1237 \times 27\,x_1 + 4563 \equiv 0 \ (mod.\ 27 \times 25),$$

oder, wenn man durch 27 dividirt,

$$1237\,x_1 + 169 \equiv 0 \ (mod.\ 25).$$

Ersetzt man hierin die Coefficienten durch ihre kleinsten Reste, so folgt

$$12\,x_1 - 6 \equiv 0 \ (mod.\ 25).$$

Da 6 prim zum Modul ist, so darf man durch 6 dividiren, und erhält

$$2\,x_1 - 1 \equiv 0 \ (mod.\ 25),$$

oder

$$x_1 = \frac{1 + 25\,y}{2}.$$

Der Werth $y = 1$ liefert $x_1 = 13$, die gesuchte Wurzel ist daher

$$x = 7 + 27 \times 13 = 358.$$

290. Auf die Aufgabe, die wir soeben gelöst haben, führt man folgende zurück: Eine Zahl N zu bestimmen, welche in Beziehung auf gegebene Moduln M, M_1, M_2, ... gegebene Reste a, a_1, a_2, ... hat.

Die gesuchte Zahl N muss den Congruenzen

$$(1).\quad N \equiv a\ (mod.\ M)\ ,\ N \equiv a_1\ (mod.\ M_1)\ ,\ N \equiv a_2\ (mod.\ M_2)\ ,\ \ldots$$

genügen; die erste derselben liefert

$$N = a + Mx,$$

und damit die so bestimmte Zahl N auch die zweite der Congruenzen (1) befriedige, muss

$$a + Mx \equiv a_1\ (mod.\ M_1) \text{ oder } Mx + (a - a_1) \equiv 0\ (mod.\ M_1)$$

sein. Wenn der grösste gemeinschaftliche Divisor d der Zahlen M und M_1 nicht auch in $a - a_1$ aufgeht, so ist die vorgelegte Aufgabe unlösbar; im entgegengesetzten Falle lässt sich die vorhergehende Congruenz in folgender Weise schreiben

$$\frac{M}{d}\, x + \frac{a - a_1}{d} \equiv 0\ \left(mod.\ \frac{M_1}{d}\right).$$

und wenn α ihre Wurzel bezeichnet, so ist diese Congruenz nur durch die in

$$x = \alpha + \frac{M_1}{d}\, x_1$$

enthaltenen Werthe von x zu befriedigen, in welcher Formel x_1 eine unbestimmte Grösse bedeutet. Setzt man

$$a + M\alpha = a^{(1)},$$

so erhält man folgenden Ausdruck von N:

$$N = a^{(1)} + \frac{MM_1}{d}\, x_1.$$

Soll dieser Werth von N auch der dritten der Congruenzen (1) genügen, so muss

$$a^{(1)} + \frac{MM_1}{d}\, x_1 \equiv a_2\ (mod.\ M_2),$$

oder

$$\frac{MM_1}{d}\, x_1 + (a^{(1)} - a_2) \equiv 0\ (mod.\ M_2)$$

sein. Wenn der grösste gemeinschaftliche Divisor d_1 der Zahlen $\frac{MM_1}{d}$ und M_2 nicht auch in $a^{(1)} - a_2$ aufgeht, so ist die vorhergehende Congruenz unmöglich; im entgegengesetzten Falle lässt sie sich auf die Form

$$\frac{MM_1}{dd_1} x_1 + \frac{a^{(1)} - a_2}{d_1} \equiv 0 \left(mod. \frac{M_2}{d_1}\right)$$

bringen, und wenn α_1 ihre Wurzel ist, so muss man

$$x_1 = \alpha_1 + \frac{M_2}{d_1} x_2$$

setzen, wo x_2 eine unbestimmte Grösse bezeichnet. Macht man dann

$$a^{(1)} + \frac{M M_1}{d} \alpha_1 = a^{(2)} ,$$

so ist

$$N = a^{(2)} + \frac{M M_1 M_2}{dd_1} x_2 .$$

In dieser Weise kann man fortfahren, bis alle vorgelegten Congruenzen erschöpft sind. Gelangt man dabei nie zu einer unmöglichen Congruenz, so ergiebt sich für N ein Ausdruck von der Form

$$N = A + \mu X ,$$

worin X eine unbestimmte Grösse und μ das kleinste gemeinschaftliche Vielfache der Moduln M, M_1, M_2, . . . bezeichnet.

291. Der Fall, in welchem die Auflösung von m Congruenzen ersten Grades mit m Unbekannten gefordert wird, lässt sich mittels der vorhergehenden Betrachtungen behandeln. Die gegebenen Congruenzen, deren Lösungssysteme bestimmt werden sollen, seien folgende:

$$(1). \left\{ \begin{array}{l} a_0 \quad x + b_0 \quad y + c_0 \quad z + \cdots + k_0 \quad u + l_0 \quad \equiv 0 \\ a_1 \quad x + b_1 \quad y + c_1 \quad z + \cdots + k_1 \quad u + l_1 \quad \equiv 0 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{m-1} x + b_{m-1} y + c_{m-1} z + \cdots + k_{m-1} u + l_{m-1} \equiv 0 \end{array} \right\} (mod. M).$$

Die Werthe irgend einer der Unbekannten hängen von einer leicht zu bildenden linearen Congruenz ab. Die Theorie der Gleichungen ersten Grades setzt uns nämlich in den Stand, m ganze Zahlen ξ_0, ξ_1, . . ., ξ_{m-1} zu ermitteln, welche sämmtlich prim zum Modul sind und den $m - 1$ Gleichungen

$$(2). \quad \left\{ \begin{array}{l} b_0 \xi_0 + b_1 \xi_1 + \cdots + b_{m-1} \xi_{m-1} = 0 , \\ c_0 \xi_0 + c_1 \xi_1 + \cdots + c_{m-1} \xi_{m-1} = 0 , \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad , \\ k_0 \xi_0 + k_1 \xi_1 + \cdots + k_{m-1} \xi_{m-1} = 0 \end{array} \right.$$

genügen. Werden nun die Congruenzen (1) beziehungsweise mit

$\xi_0, \xi_1, \ldots, \xi_{m-1}$ multiplicirt und sodann addirt, so ergiebt sich

$$a x + l \equiv 0 \ (mod.\ M)\ ,$$

wo der Kürze wegen

$$a_0 \xi_0 + a_1 \xi_1 + \cdots + a_{m-1} \xi_{m-1} = a\ ,$$
$$l_0 \xi_0 + l_1 \xi_1 + \cdots + l_{m-1} \xi_{m-1} = l$$

gesetzt ist.

In derselben Weise kann man hinsichtlich der Unbekannten $y, z, \ldots$ verfahren. Man erhält dadurch m Congruenzen, von denen jede nur eine Unbekannte enthält, und welche alle Lösungen des vorgelegten Systems zulassen. Man kann aber nicht behaupten, dass umgekehrt auch alle Lösungen des neu erhaltenen Systems das vorgelegte System befriedigten. In der Praxis ist es im Allgemeinen einfacher, die Unbekannten der Reihe nach zu eliminiren und das System (1) durch ein anderes zu ersetzen, in welchem jede Congruenz eine Unbekannte weniger als die vorhergehende enthält.

Beispiel. — Die gegebenen Congruenzen seien

$$(1).\qquad \left.\begin{cases} 3x + 5y + \ \ z \equiv 4 \\ 2x + 3y + 2z \equiv 7 \\ 5x + \ \ y + 3z \equiv 6 \end{cases}\right\} (mod.\ 12).$$

(Dasselbe Beispiel hat Gauss in den Disquisitiones 37 gewählt). Nimmt man aus der ersten Congruenz den Werth von z und substituirt ihn in die beiden andern, so erhält man das neue System

$$(2).\qquad \left.\begin{cases} z \equiv 4 - 3x - 5y \\ 4x + 7y \equiv 1 \\ 4x + 2y \equiv 6 \end{cases}\right\} (mod.\ 12).$$

Wird jetzt x aus den beiden letzten Congruenzen eliminirt, so entsteht das dritte System

$$(3).\qquad \left.\begin{cases} z \equiv 4 - 3x - 5y \\ 4x \equiv 1 - 7y \\ 5y \equiv \ \ -5 \end{cases}\right\} (mod.\ 12).$$

Die letzte Congruenz des Systems (3) besitzt nur eine Wurzel, nämlich -1 oder 11. Dann liefert die zweite der Congruenzen (3)

$$4x \equiv 8 \ (mod.\ 12),$$

oder

$$x \equiv 2 \ (mod.\ 3)\ ,$$

und daraus ergeben sich für x die vier Werthe

$$x = 2,\ 5,\ 8,\ 11.$$

Da $y = -1$ ist, so reducirt sich die erste der Congruenzen (3) auf

$$z \equiv 9 - 3x,$$

und diese liefert die den Werthen von x entsprechenden Werthe von z, nämlich

$$z = 3,\ 6,\ 9,\ 0.$$

Ueber die Anzahl der Wurzeln der Congruenz $x^2 - 1 \equiv 0$ (*mod. M*).

292. Damit das Produkt $(x+1)(x-1)$ durch M theilbar sei, ist erforderlich und hinreichend, dass $x - 1$ alle diejenigen Primfactoren von M enthalte, welche nicht in $x + 1$ aufgehen. Ausserdem können $x - 1$ und $x + 1$ nur die Divisoren 1 und 2 gemeinschaftlich haben, da ihre Differenz gleich 2 ist. Um also die Congruenz

$$(1).\qquad x^2 - 1 \equiv 0 \ (mod.\ M)$$

aufzulösen, genügt es, auf alle möglichen Arten

$$M = AB$$

zu setzen, wo A und B entweder prim zu einander sind, oder als grössten gemeinschaftlichen Divisor 2 haben, und sodann die Werthe von x zu bestimmen, welche gleichzeitig den beiden Congruenzen

$$(2).\qquad x + 1 \equiv 0 \ (mod.\ A)\ ,\ x - 1 \equiv 0 \ (mod.\ B)$$

genügen.

Aus der ersten dieser Congruenzen folgt

$$(3).\qquad x = -1 + At,$$

wo t eine unbestimmte Grösse bedeutet, und durch Einsetzung dieses Werthes in die zweite der Congruenzen (2) ergiebt sich

$$(4).\qquad At - 2 \equiv 0 \ (mod.\ B).$$

Da der grösste gemeinschaftliche Divisor von A und B der Voraussetzung nach 1 oder 2 ist, so ist die Congruenz (4) immer möglich. Sind A und B prim zu einander, so besitzt dieselbe nur eine Wurzel, und die Formel (3) liefert für x gleichfalls nur einen Werth. Haben aber A und B den Divisor 2 gemeinschaft-

lich, so lässt sich die Congruenz (4) durch 2 dividiren und geht über in

(5). $$\frac{A}{2}\,t - 1 \equiv 0 \left(mod.\ \frac{B}{2}\right).$$

Die Werthe von t, welche dieser Congruenz genügen, sind durch die Formel

$$t = t_0 + \frac{B}{2}\,u$$

gegeben, in welcher t_0 eine zwischen 0 und $\frac{B}{2}$ enthaltene bestimmte Zahl und u eine neue Veränderliche bezeichnet. Dann hat die Congruenz (4) die beiden Wurzeln

$$t_0\ ,\ t_0 + \frac{B}{2}\,,$$

und die Formel (3) liefert die entsprechenden Werthe von x:

$$-1 + At_0\ ,\ -1 + At_0 + \frac{M}{2}\,.$$

Es ist jetzt wichtig zu untersuchen, ob eine der Wurzeln der vorgelegten Congruenz durch zwei verschiedene Zerlegungen des Moduls M:

$$M = AB\ ,\ M = A'B'$$

erhalten werden kann. Wir bezeichnen mit $\frac{a}{b}$ den irreductibeln Bruch, welcher den beiden Brüchen

$$\frac{A}{B'}\ ,\ \frac{A'}{B}$$

äquivalent ist; dass letztere einander gleich sind, geht aus der Annahme $AB = A'B'$ hervor. Es ist dann

$$A = \lambda a\ ,\ A' = \mu a\,,$$
$$B' = \lambda b\ ,\ B = \mu b\,,$$

folglich

$$A' = \frac{\mu}{\lambda}\,A\,,\ B' = \frac{\lambda}{\mu}\,B\,,$$

wo λ und μ ganze Zahlen bedeuten. Wenn aber die betrachteten Zerlegungen ein und dieselbe Wurzel x der Congruenz (1) liefern, so gehen die Zahlen A und B' oder A' und B beziehungsweise in $x + 1$ und $x - 1$ auf; sie haben daher als grössten gemeinschaftlichen Divisor 1 oder 2, d. h. jede der Zahlen λ und μ ist gleich 1 oder 2. Daraus geht hervor, dass die Zerlegungen

$$M = \frac{1}{2} A \times 2 B\ ,\ M = 2 A \times \frac{1}{2} B$$

die einzigen sind, welche eine durch die Zerlegung $M = AB$ bereits gelieferte Wurzel x geben können.

Dies vorausgesetzt, ist es leicht, die Anzahl N der verschiedenen Wurzeln der Congruenz (1) zu bestimmen.

Wir setzen den Modul M zunächst als ungerade voraus und bezeichnen die Anzahl seiner ungeraden Primfactoren mit n. In diesem Falle liefern die Zerlegungen $M = AB$ nothwendig verschiedene Wurzeln, und es handelt sich also nur darum, die Anzahl dieser Zerlegung zu ermitteln. Was nun die Bildung von A betrifft, so kann man erstens $A = 1$ annehmen; ferner kann man A aus einem einzigen der n Primfactoren von M bestehen lassen und erhält dadurch n verschiedene Zerlegungen; weiter erhält man $\frac{n(n-1)}{1.2}$ Zerlegungen, wenn man A aus zwei Primfactoren von M zusammensetzt, u. s. w. Danach ist

$$N = 1 + \frac{n}{1} + \frac{n(n-1)}{1.2} + \cdots + \frac{n}{1} + 1$$

oder

$$N = 2^n.$$

Zweitens nehmen wir an, der Modul M sei das Doppelte einer ungeraden Zahl, welche wieder aus n ungleichen Primfactoren bestehen möge. Wir betrachten die Zerlegung

$$M = AB,$$

in welcher A gerade, B ungerade ist. Von allen übrigen Zerlegungen ist

$$M = \frac{1}{2} A \times 2 B$$

die einzige, welche dieselbe Wurzel wie die erstgenannte liefern könnte, und wir behaupten, dass sie sie wirklich liefert. Die Wurzel, welche der ersten Zerlegung entspricht, ist nämlich durch die Formeln

$$x = -1 + At\ ,\ At - 2 \equiv 0\ (mod.\ B)$$

bestimmt. Da nun A gerade, B ungerade ist, so kann man schreiben

$$x = -1 + \frac{A}{2} \cdot 2t\ ,\ \frac{A}{2} \cdot 2t - 2 \equiv 0\ (mod.\ 2B),$$

und der hierdurch bestimmte Werth von x entspricht augen-

scheinlich auch der zweiten Zerlegung. Daraus folgt, dass N die Anzahl der Zerlegungen von $\frac{M}{2}$ in zwei Factoren ist, welche prim zu einander sind, und man hat, wie im ersten Falle,

$$N = 2^n.$$

Endlich setzen wir voraus, M sei durch die Potenz 2^ϱ von 2 theilbar, deren Exponent $\varrho > 1$ ist. Die Anzahl der ungleichen (ungeraden) Primfactoren von $\frac{M}{2^\varrho}$ bezeichnen wir wieder mit n. In diesem Falle kann man jede Zerlegung

$$M = AB$$

bei Seite lassen, in welcher eine der Zahlen A und B ungerade ist. Wäre nämlich A gerade, B ungerade, so würde das im vorigen Falle angewandte Schlussverfahren zeigen, dass die Wurzel, welche der Zerlegung AB entspricht, auch durch die Zerlegung $\frac{A}{2} \times 2B$ gegeben wird. Eine Zerlegung von M in zwei gerade Factoren liefert zwei Wurzeln x, welche nothwendig von den durch eine andere Zerlegung dieser Art erhaltenen verschieden sind; denn in jeder Zerlegung müssen die Factoren als grössten gemeinschaftlichen Divisor 2 enthalten. Um also alle brauchbaren Zerlegungen von M zu erhalten, hat man diejenigen von $\frac{M}{2^\varrho}$ zu bilden und 2 in den ersten, $2^{\varrho-1}$ in den zweiten, sodann umgekehrt $2^{\varrho-1}$ in den ersten, 2 in den zweiten Factor einzuführen. Wenn $\varrho = 2$ ist, so gehen diese beiden letzten Operationen offenbar in einander ein.

Aus der vorstehenden Betrachtung ergiebt sich Folgendes:

Ist $\varrho = 2$, d. h. M durch 4, aber nicht durch 8 theilbar, so hat man

$$N = 2^{n+1}.$$

Ist $\varrho > 2$, d. h. M durch 8 theilbar, so hat man

$$N = 2^{n+2}.$$

Dieser Schluss bleibt auch richtig, wenn $M = 2^\varrho$ ist; in diesem Falle lässt $\frac{M}{2^\varrho}$ nur die Zerlegung 1×1 zu.

Man beachte, dass je zwei Wurzeln der Congruenz (1) **conjugirt**, d. h. gleich, aber mit entgegengesetzten Zeichen behaf-

tet sind. Es liegt auf der Hand, dass zwei conjugirte Wurzeln durch zwei Zerlegungen wie AB, BA entstehen.

Zusatz. — Die Congruenz

$$x^2 - 1 \equiv 0 \pmod{M}$$

besitzt nur ein Paar conjugirter Wurzeln in einem der drei folgenden Fälle: 1° wenn M eine Potenz einer ungeraden Primzahl ist; 2° wenn M das Doppelte einer solchen Potenz ist; 3° wenn M gleich 4 ist. In jedem andern Falle hat die Congruenz eine gerade Anzahl Paare conjugirter Wurzeln.

Dieser Zusatz ergiebt sich unmittelbar aus den Formeln, durch welche wir die Zahl N in den oben untersuchten verschiedenen Fällen ausgedrückt haben.

Beispiel. — Für $M = 24$ giebt es vier brauchbare Zerlegungen, nämlich

$$A = 2\,,\ 12\,,\ 4\,,\ 6\,,$$
$$B = 12\,,\ 2\,,\ 6\,,\ 4\,.$$

Die Congruenz

$$x^2 - 1 \equiv 0 \pmod{24}$$

hat daher acht Wurzeln:

Die Zerlegung 2×12 liefert die Wurzeln 1, 13,
Die Zerlegung 12×2 „ „ „ 23, 11,
Die Zerlegung 4×6 „ „ „ 7, 19,
Die Zerlegung 6×4 „ „ „ 17, 5.

Der Fermat'sche Satz.

293. Der Fermat'sche Satz ist einer der wichtigsten Sätze der Theorie, mit der wir uns jetzt beschäftigen, und wir halten es für nützlich, die verschiedenen dafür gegebenen Beweise hier mitzutheilen. Der Satz ist folgender:

Lehrsatz. — Wenn die ganze Zahl a durch die Primzahl p nicht theilbar ist, so ist die Differenz $a^{p-1} - 1$ durch p theilbar, d. h. man hat

$$a^{p-1} \equiv 1 \pmod{p}.$$

Erster Beweis. — Da a und p der Voraussetzung nach prim zu einander sind, so liefern die Zahlen

(1). $a\,,\,2a\,,\,3a\,,\ldots,\,(p-1)\,a$

nach No. 283, wenn man sie durch p dividirt, in irgend einer Reihenfolge beziehungsweise die Reste

(2). $1\,,\,2\,,\,3\,,\ldots,\,(p-1).$

Das Produkt der Zahlen (1) muss daher nach dem Modul p dem Produkte der Zahlen (2) congruent sein, d. h. es ist

$$1\,.\,2\,.\,3\,\ldots\,(p-1)\,(a^{p-1}-1)\equiv 0\ (mod.\ p).$$

Man kann diese Congruenz durch das Produkt $1\,.\,2\,.\,3\ldots(p-1)$, welches prim zum Modul ist, dividiren, und erhält

$$a^{p-1}-1\equiv 0\ (mod.\ p).$$

Zweiter Beweis. — Erhebt man das Binom

$$(a-1)+1\,,$$

welches den Werth a hat, auf die p^{te} Potenz, so erhält man

$$a^p=(a-1)^p+\frac{p}{1}\,(a-1)^{p-1}+\cdots$$

$$+\frac{p\,(p-1)\ldots(p-k+1)}{1.2\ldots k}\,(a-1)^{p-k}+\cdots+1.$$

Im zweiten Gliede dieser Formel sind alle Terme, mit Ausnahme des ersten und des letzten, durch p theilbar; denn der Coefficient

$$\frac{p\,(p-1)\ldots(p-k+1)}{1.2\ldots k}$$

ist eine ganze Zahl, und diese ganze Zahl enthält augenscheinlich den Factor p, wenn $k<p$ ist. Man hat daher

$$a^p\equiv(a-1)^p+1\ (mod.\ p),$$

oder, wenn beiderseits a subtrahirt wird,

$$a^p-a\equiv(a-1)^p-(a-1)\ (mod.\ p).$$

Diese Formel zeigt, dass die Differenz a^p-a sich nur um ein Vielfaches von p ändert, wenn man a um eine Einheit verringert. Dasselbe muss daher der Fall sein, wenn $2,\ 3,\ldots,\ a$ Einheiten von a subtrahirt werden; es ist folglich

$$a^p-a\equiv 0\ (mod.\ p).$$

Diese Congruenz darf durch a dividirt werden, da a prim zum Modul p ist, und es ergiebt sich

$$a^{p-1}-1\equiv 0\ (mod.\ p).$$

Dritter Beweis. — Bedeuten u und v irgend welche ganze Zahlen, so hat man

$$(u+v)^p = u^p + \frac{p}{1} u^{p-1} v + \cdots$$
$$+ \frac{p(p-1)\ldots(p-k+1)}{1.2\ldots k} u^{p-k} v^k + \cdots + v^p.$$

Da nun im zweiten Gliede dieser Formel, wie wir uns soeben überzeugt haben, alle Terme, mit Ausnahme des ersten und des letzten, durch p theilbar sind, so ist

$$(u+v)^p \equiv u^p + v^p \ (mod.\ p).$$

Es seien jetzt $\alpha_1, \alpha_2, \ldots, \alpha_a$ ganze Zahlen. Nach der vorhergehenden Formel ist

$$\left.\begin{array}{ll} (\alpha_1+\alpha_2+\cdots+\alpha_a)^p \equiv \alpha_1^p + (\alpha_2+\cdots+\alpha_a)^p \\ (\alpha_2+\alpha_3+\cdots+\alpha_a)^p \equiv \alpha_2^p + (\alpha_3+\cdots+\alpha_a)^p \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ (\alpha_{a-1}+\alpha_a)^p \equiv \alpha_{a-1}^p + \alpha_a^p \end{array}\right\} mod.\ p),$$

und durch Addition ergiebt sich hieraus

$$(\alpha_1+\alpha_2+\cdots+\alpha_a)^p \equiv \alpha_1^p + \alpha_2^p + \cdots + \alpha_a^p \ (mod.\ p).$$

In dieser Formel lassen wir jede der Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_a$ sich auf die Einheit reduciren und erhalten

$$a^p \equiv a \ (mod.\ p),$$

oder, wenn durch a dividirt wird,

$$a^{p-1} \equiv 1 \ (mod.\ p).$$

Der Wilson'sche Satz.

294. Lehrsatz. — Wenn p eine Primzahl bezeichnet, so ist die Summe $1.2.3\ldots(p-1)+1$ durch p theilbar, d. h. man hat

$$1.2.3\ldots(p-1) \equiv -1 \ (mod.\ p).$$

Erster Beweis. — Es sei a eine beliebige Zahl der Reihe

(1). $\quad 1, 2, 3, \ldots, (p-1).$

Bilden wir dann die Produkte

(2). $\quad a, 2a, 3a, \ldots (p-1)a,$

so ist in der Reihe (2) stets ein, aber auch nur ein Term vorhanden, welcher der Einheit congruent ist; dieser Term möge αa sein, so dass

$$\alpha a \equiv 1 \ (mod.\ p).$$

Die Zahlen a und α sind ungleich, wofern nicht a gleich 1 oder gleich $p - 1$ ist. Hat man nämlich $\alpha = a$, so ist

$$a^2 - 1 = (a + 1)\ (a - 1)$$

durch p theilbar, und da p eine Primzahl ist, so muss entweder $a - 1$ oder $a + 1$ p als Factor enthalten. Nun ist aber

$$a < p, \text{ folglich } a = 1 \text{ oder } a = p - 1.$$

Danach können die Zahlen

$$2\ ,\ 3\ ,\ 4\ ,\ \ldots\ ,\ (p - 2)$$

in Gruppen von je zweien in der Weise vertheilt werden, dass das Produkt der Zahlen jeder Gruppe nach dem Modul p der Einheit congruent ist.

Durch Multiplication aller auf diese Weise erhaltenen Congruenzen ergiebt sich

$$2\ .\ 3\ .\ 4 \ldots (p-2) \equiv 1 \ (mod.\ p).$$

Wird diese Congruenz mit $p - 1$ multiplicirt, so folgt

$$1\ .\ 2\ .\ 3\ .\ 4 \ldots (p - 1) \equiv p - 1 \ (mod.\ p),$$

oder

$$1\ .\ 2\ .\ 3\ .\ 4 \ldots (p - 1) + 1 \equiv 0 \ (mod.\ p), \text{ w. z. b. w.}$$

Dieser Satz ist besonders deshalb bemerkenswerth, weil er eine Eigenschaft ausdrückt, welche nur die Primzahlen besitzen. Denn wenn p eine zusammengesetzte Zahl und ϑ einer der Divisoren von p ist, so geht ϑ in das Produkt $1\ .\ 2\ .\ 3 \ldots (p - 1)$ auf: folglich kann die Summe $1\ .\ 2\ .\ 3 \ldots (p - 1) + 1$ nicht durch ϑ, also auch nicht durch p theilbar sein.

Zusatz. — Jede Primzahl p von der Form $4n + 1$ ist die Summe zweier Quadrate.

Nach dem vorhergehenden Satze geht p in die Summe

$$(1.2.3 \ldots 2n)\ [(2n + 1) \ldots 4n] + 1$$

auf. Nun sind aber die Zahlen

$$2n + 1\ ,\ 2n + 2\ ,\ \ldots\ ,\ 4n$$

nach dem Modul p beziehungsweise den Zahlen

$$-2n\ ,\ -(2n-1)\ ,\ \ldots\ ,\ -1$$

congruent; folglich ist das Produkt der einen congruent dem Produkte der andern. Da ausserdem die Anzahl der Factoren gerade ist, so kann man ihre Zeichen ändern und erhält

$$(1.2.3\ldots 2n)^2 + 1 \equiv 0 \ (mod.\ p);$$

p geht danach in die Summe zweier Quadrate auf; mithin ist (No. 15) p selbst die Summe zweier Quadrate.

Anmerkung. Es giebt keine Zahl von der Form $4n + 3$, welche die Summe zweier Quadrate wäre. Jedes gerade Quadrat ist nämlich von der Form $4n$, jedes ungerade von der Form $4n + 1$; folglich hat die Summe zweier Quadrate, welche prim zu einander sind, stets eine der beiden Formen $4n + 1$ und $4n + 2$.

Zweiter Beweis. — Man kann den Wilson'schen Satz auch mittels der in No. 152 hergeleiteten Formel

$$\Delta^n u_0 = u_n - \frac{n}{1} u_{n-1} + \frac{n(n-1)}{1.2} u_{n-2} - \cdots + (-1)^n u_0$$

beweisen, welche die n^{te} Differenz des Terms u_0 der Reihe

$$u_0 \ , \ u_1 \ , \ u_2 \ , \ u_3 \ , \ldots$$

ausdrückt. Wird allgemein

$$u_\mu = (x + \mu)^n$$

vorausgesetzt, so hat man

$$\Delta^n u_\mu = 1.2.3\ldots n,$$

und unsere allgemeine Formel geht über in

$$1.2.3\ldots n = (x+n)^n - \frac{n}{1}(x+n-1)^n$$
$$+ \frac{n(n-1)}{1\cdot 2}(x+n-2)^n - \cdots + (-1)^n x^n.$$

Ist jetzt $x = 1$ und $n = p - 1$, wo p eine Primzahl bedeutet, so ergiebt sich

$$1.2.3\ldots(p-1) = p^{p-1} - \frac{p-1}{1}(p-1)^{p-1}$$
$$+ \frac{(p-1)(p-2)}{1\cdot 2}(p-2)^{p-1} - \cdots$$
$$- \frac{p-1}{1} 2^{p-1} + 1^{p-1}.$$

Ausserdem hat man

$$0 = (1-1)^{p-1} = 1 - \frac{p-1}{1} + \frac{(p-1)(p-2)}{1\cdot 2} - \cdots + 1,$$

folglich

$$1.2.3\ldots(p-1)+1 = p^{p-1} - \frac{p-1}{1}\left[(p-1)^{p-1}-1\right] + \frac{(p-1)(p-2)}{1.2}\left[(p-2)^{p-1}-1\right] - \cdots - \frac{p-1}{1}\left(2^{p-1}-1\right).$$

Im zweiten Gliede dieser Formel ist der erste Term eine Potenz von p, und alle folgenden Terme sind nach dem Fermat'schen Satze durch p theilbar; es ist daher

$$1.2.3\ldots(p-1)+1 \equiv 0 \ (mod.\ p).$$

(*Anmerk. d. U.*) — Einen sehr schönen auf ganz anderen Betrachtungen beruhenden Beweis des Wilson'schen Satzes giebt Stern in seiner „Algebr. Analysis", Note VII.

Der verallgemeinerte Fermat'sche Satz.

295. Der Fermat'sche Satz lässt sich auf zusammengesetzte Moduln ausdehnen; in der That ist er nur ein specieller Fall des folgenden Satzes:

Lehrsatz. — Wenn a und M relative Primzahlen sind, und $\varphi(M)$ ausdrückt, wie viele Zahlen prim zu M und nicht grösser als M sind, so ist die Differenz

$$a^{\varphi(M)} - 1$$

durch M theilbar, d. h. man hat

$$a^{\varphi(M)} - 1 \equiv 0 \ (mod.\ M).$$

Der erste der in No. 293 gegebenen Beweise lässt sich mit geringen Modificationen auf den vorliegenden Fall anwenden. Es seien

$$(1).\qquad \alpha,\ \beta,\ \gamma,\ \delta,\ \ldots,\ \omega$$

die $\varphi(M)$ Zahlen, welche prim zu M und nicht grösser als M sind. Werden dieselben mit der Zahl a, welche gleichfalls prim zu M ist, multiplicirt, so erhält man die neue Reihe

$$(2).\qquad a\alpha,\ a\beta,\ a\gamma,\ a\delta,\ \ldots,\ a\omega.$$

Betrachten wir irgend einen Term der Reihe (2), z. B. $a\alpha$, so ist der Voraussetzung nach M prim zu a und grösser als α; folglich kann kein Term der Reihe (2) durch M theilbar sein. Aus demselben Grunde kann M auch nicht in die Differenz $a(\beta-\alpha)$ zweier Terme der Reihe (2) aufgehen. Bildet man daher in Be-

ziehung auf M die kleinsten Reste der Zahlen (2), so erhält man $\varphi(M)$ verschiedene Resultate. Ausserdem sind die Zahlen (2), also auch ihre Reste prim zu M. Diese Reste stimmen daher, abgesehen von der Reihenfolge, mit den Zahlen (1) völlig überein, und da somit die Zahlen (1) beziehungsweise den Zahlen (2) congruent sind, so ist das Produkt der einen dem Produkte der andern congruent, d. h. man hat

$$\alpha\beta\gamma\ldots\omega\,[a^{\varphi(M)}-1]\equiv 0\ (mod.\ M)\ ,$$

oder, wenn man durch das Produkt $\alpha\beta\gamma\ldots\omega$, welches prim zum Modul ist, dividirt,

$$a^{\varphi(M)}-1\equiv 0\ (mod.\ M)\ .$$

Der verallgemeinerte Wilson'sche Satz.

296. Auch der Wilson'sche Satz lässt sich verallgemeinern, und zwar folgendermassen:

Lehrsatz. — Bezeichnet P das Produkt der $\varphi(M)$ Zahlen, welche prim zu M und nicht grösser als M sind, so hat man

$$P\equiv\mp 1\ (mod.\ M)\ .$$

Es ist nämlich

$$P\equiv -1\ (mod.\ M)\ ,$$

wenn M gleich einer Potenz einer ungeraden Primzahl, oder gleich dem Doppelten einer solchen Potenz, oder gleich 4 ist; in allen übrigen Fällen hat man

$$P\equiv +1\ (mod.\ M)\ .$$

Es seien wieder

(1). $\alpha\ ,\ \beta\ ,\ \gamma\ ,\ \ldots\ ,\ \omega$

die Zahlen, welche prim zu M und nicht grösser als M sind. Bezeichnet a eine derselben, so haben die Produkte

(2). $a\alpha\ ,\ a\beta\ ,\ a\gamma\ ,\ \ldots\ ,\ a\omega\ ,$

wie wir oben sahen, in Beziehung auf den Modul M verschiedene kleinste Reste. Einer dieser Reste muss daher gleich 1, ein anderer gleich $M-1$ sein. Wir nehmen an, $a\alpha$ liefere den Rest 1; wenn a und α ungleich sind, so wollen wir sie zusammengehörige Zahlen der ersten Art nennen. Ist $\alpha=a$, so liefert das Produkt $a(M-a)$ den Rest -1 oder $M-1$, da $a\times a$ den Rest 1 liefert; wir wollen dann a und $M-a$ zusammen-

gehörige Zahlen zweiter Art nennen. Aus dieser Definition folgt, dass zwei zusammengehörige Zahlen zweiter Art ein Paar conjugirte Wurzeln der Congruenz

(3). $$x^2 - 1 \equiv 0 \ (mod.\ M)$$

ausmachen. Nun ist klar, dass das Produkt aller derjenigen Zahlen der Reihe (1), welche die Paare der zusammengehörigen Zahlen erster Art bilden, nach dem Modul M der Einheit congruent ist. Dagegen ist das Produkt der Zahlen, von denen je zwei Zusammengehörige zweiter Art sind, $(-1)^\mu$ congruent, wo μ ausdrückt, wie viele Paare conjugirter Wurzeln die Congruenz (3) besitzt. Man hat daher

$$P \equiv (-1)^\mu \ (mod.\ M) .$$

Ist jetzt $M = p^\nu$, oder $M = 2p^\nu$, oder $M = 4$, wo p eine ungerade Primzahl bezeichnet, so ist $\mu = 1$; in allen übrigen Fällen ist μ eine gerade Zahl (No. 292). Man hat daher

$$P \equiv -1 \ (mod.\ M)$$

in den drei Fällen $M = p^\nu$, $= 2p^\nu$, $= 4$, und

$$P \equiv +1 \ (mod.\ M) ,$$

wenn der Modul M keine dieser drei Formen hat.

Anmerkung. — Um die mit einer Zahl a zusammengehörige Zahl zu bestimmen, genügt es, die Wurzel der Congruenz

$$ax - 1 \equiv 0 \ (mod.\ M)$$

zu suchen, oder die unbestimmte Gleichung

$$ax - My = 1$$

in ganzen Zahlen aufzulösen.

Man kann sich auch des verallgemeinerten Fermat'schen Satzes bedienen. Da nämlich

$$a^{\varphi(M)} \equiv 1 \ (mod.\ M)$$

ist, so ist die gesuchte Zahl offenbar der Rest der Potenz

$$a^{\varphi(M)-1} .$$

Congruenzen, deren Modul eine Primzahl ist.

297. Eine Congruenz

$$A_0 x^m + A_1 x^{m-1} + \cdots + A_{m-1} x + A_m \equiv 0 \ (mod.\ p) ,$$

deren Modul p als Primzahl vorausgesetzt wird, und deren Coefficienten $A_0, A_1, \ldots$ zwischen 0 und p oder zwischen $-\frac{p}{2}$ und

$+\frac{p}{2}$ liegende ganze Zahlen sind, kann immer durch eine andere ersetzt werden, in welcher der erste Term den Coefficienten Eins hat. Es sei nämlich A' die mit A_0 zusammengehörige Zahl, d. h. eine solche Zahl, dass man

$$A_0 A' \equiv 1 \pmod{p}$$

hat; ferner mögen

$$P_1 \ , \ P_2 \ , \ \ldots \ , \ P_m$$

die Reste der Produkte

$$A' A_1 \ , \ A' A_2 \ , \ \ldots \ , \ A' A_m$$

bezeichnen. Multiplicirt man alle Terme der vorgelegten Congruenz, mit Ausnahme des ersten, mit $A_0 A'$, so nimmt dieselbe die Form an:

$$A_0 (x^m + P_1 x^{m-1} + P_2 x^{m-2} + \cdots + P_{m-1} x + P_m) \equiv 0 \pmod{p},$$

und wenn jetzt durch die Zahl A_0, welche prim zum Modul ist, dividirt wird, so ergiebt sich

$$x^m + P_1 x^{m-1} + P_2 x^{m-2} + \cdots + P_{m-1} x + P_m \equiv 0 \pmod{p}.$$

298. Die Congruenzen, deren Modul eine Primzahl ist, besitzen eine äusserst wichtige Eigenschaft, welche der folgende Satz ausdrückt:

Lehrsatz. — Eine nicht identische Congruenz, deren Modul eine Primzahl ist, kann nicht mehr Wurzeln haben, als ihr Grad Einheiten enthält.

Es sei

$$f(x) \equiv 0 \pmod{p} \tag{1}$$

eine Congruenz m^{ten} Grades, der Modul p eine Primzahl. $f(x)$ bezeichnet der Kürze wegen das Polynom

$$f(x) = A_0 x^m + A_1 x^{m-1} + \cdots + A_{m-1} x + A_m,$$

dessen Coefficienten ganze Zahlen sind, die zwischen 0 und p oder zwischen $-\frac{p}{2}$ und $+\frac{p}{2}$ liegen.

Wir stellen jetzt durch $a_1, a_2, \ldots, a_m$ irgendwelche ganze Zahlen dar und setzen, wie in No. 45,

$$\left\{\begin{aligned} f(x) &= (x-a_1)\, f_1(x) + R_1 \ , \\ f_1(x) &= (x-a_2)\, f_2(x) + R_2 \ , \\ f_2(x) &= (x-a_3)\, f_3(x) + R_3 \ , \\ &\cdots\cdots\cdots\cdots , \\ f_{m-1}(x) &= (x-a_m)\, f_m(x) + R_m \ , \end{aligned}\right. \tag{2}$$

wo $R_1, R_2, \ldots, R_m$ von x unabhängige Grössen sind. Darauf addiren wir alle diese Identitäten, nachdem wir sie beziehungsweise mit den m Factoren

$$1 \; , \; x-a_1 \; , \; (x-a_1)(x-a_2) \; , \; \ldots \; , \; (x-a_1) \ldots (x-a_{m-1})$$

multiplicirt haben, und erhalten, wenn $f_m(x)$ durch seinen Werth A_0 ersetzt wird,

$$(3). \quad \begin{cases} f(x) = A_0 (x-a_1)(x-a_2)\ldots(x-a_m) \\ \qquad + R_m (x-a_1)(x-a_2)\ldots(x-a_{m-1}) + \cdots \\ \qquad + R_3 (x-a_1)(x-a_2) + R_2 (x-a_1) + R_1 \, . \end{cases}$$

Besitzt nun die vorgelegte Congruenz eine Wurzel, die etwa gleich a_1 sei, so hat man

$$R_1 \equiv 0 \; (mod. \; p) \, ,$$

und die Congruenz (1) lässt sich den Identitäten (2) zufolge auf die Form bringen:

$$(x-a_1) f_1(x) \equiv 0 \; (mod. \; p) \, .$$

Da der Modul p eine Primzahl ist, so kann das Produkt $(x-a_1) f_1(x)$ nach diesem Modul nur dann congruent Null sein, wenn einer seiner Factoren durch p theilbar ist. Hat also die vorhergehende Congruenz Wurzeln, die von a_1 verschieden sind, so müssen dieselben der Congruenz

$$(4). \qquad f_1(x) \equiv 0 \; (mod. \; p)$$

angehören. Besitzt die Congruenz (4) keine einzige Wurzel, so hat die vorgelegte Congruenz nur die Wurzel a_1. Im entgegengesetzten Falle sei a_2 einer der Werthe von x, welche der Congruenz (4) genügen; dann ist

$$R_2 \equiv 0 \; (mod. \; p) \, ,$$

und die Congruenz (4) nimmt der Identitäten (2) wegen die Form an:

$$(x-a_2) f_2(x) \equiv 0 \; (mod. \; p) \, .$$

Das eben angewandte Schlussverfahren lehrt weiter, dass, wenn diese Congruenz von a_2 verschiedene Wurzeln besitzt, dieselben der Congruenz

$$f_2(x) \equiv 0 \; (mod. \; p)$$

angehören.

Allgemein ergiebt sich Folgendes:

Hat jede der Congruenzen

$$f(x) \equiv 0 \; , \; f_1(x) \equiv 0 \; , \; \ldots \; , \; f_{m-\mu-1}(x) \equiv 0 \; (mod. \; p)$$

eine Wurzel, die Congruenz

$$f_{m-\mu}(x) \equiv 0 \ (mod.\ p)$$

aber nicht, so besitzt die vorgelegte Congruenz $m-\mu$ Wurzeln. Nehmen wir an, es seien $a_1, a_2, \ldots, a_{m-\mu}$ diese Wurzeln, so ist

$$R_1 \equiv 0 \quad , \quad R_2 \equiv 0 \quad , \quad \ldots \quad , \quad R_{m-\mu} \equiv 0 \ (mod.\ p) \ ,$$

und die Formel (3) liefert

(5). $$f(x) \equiv (x-a_1)(x-a_2) \ldots (x-a_{m-\mu})\, F(x) \ (mod.\ p) \ ;$$

darin bezeichnet $F(x)$ eine ganze Function μ^{ten} Grades, die so beschaffen ist, dass die Congruenz

$$F(x) \equiv 0 \ (mod.\ p)$$

keine Wurzel besitzt.

Wenn die Zahl μ gleich Null ist, so reducirt sich die Function $F(x)$ auf die Constante A_0, und die Formel (3) liefert

(6). $$f(x) \equiv A_0 (x-a_1)(x-a_2) \ldots (x-a_m) \ (mod.\ p) \ .$$

Daraus folgt, dass die vorgelegte Congruenz nur die m Zahlen a_1, $a_2, \ldots, a_m$ zu Wurzeln haben kann.

Zusatz. — Wenn die Congruenz m^{ten} Grades

$$f(x) \equiv 0 \ (mod.\ p)$$

durch mehr als m Werthe von x befriedigt wird, so ist sie nothwendig identisch.

299. Wir wollen jetzt eine sehr wichtige Folgerung aus dem eben hergeleiteten Satze ziehen.

Lehrsatz. — Wenn $f(x)$ und $F(x)$ ganze Functionen bezeichnen, deren Coefficienten ganze Zahlen und deren Grade kleiner als die Primzahl p sind, und wenn ferner $f(x)$ in die Function $x^{p-1}-1+p\,F(x)$ aufgeht, so besitzt die Congruenz

$$f(x) \equiv 0 \ (mod.\ p)$$

genau so viele Wurzeln, als ihr Grad Einheiten enthält.

Nach dem Fermat'schen Satze hat nämlich die Congruenz

(1). $$x^{p-1} - 1 \equiv 0 \ (mod.\ p)$$

die $p-1$ Wurzeln

$$1 \ , \ 2 \ , \ 3 \ , \ \ldots \ , \ (p-1) \ .$$

Wenn ausserdem

(2). $$x^{p-1} - 1 + p\,F(x) = f(x)\, f_1(x)$$

ist, wo $f(x)$ und $f_1(x)$ Polynome mit ganzen Coefficienten bezeichnen, so lässt sich die Congruenz (1) auf die Form

$$f(x)\, f_1(x) \equiv 0 \ (mod.\ p)$$

bringen, und jede ihrer Wurzel gehört einer der beiden Congruenzen:

(3). $f(x) \equiv 0 \quad , \quad f_1(x) \equiv (mod.\ p)$

an. Hätte jetzt eine der Congruenzen (3) weniger Wurzeln, als ihr Grad Einheiten enthält, so müsste die andere mehr Wurzeln besitzen, als in ihrem Grade Einheiten enthalten sind. Das ist aber unmöglich, der vorliegende Satz also bewiesen.

300. Der vorhergehende Satz setzt uns in den Stand, die Anzahl der Wurzeln einer Congruenz, deren Modul eine Primzahl ist, durch ein sehr einfaches Verfahren zu bestimmen. Ehe wir dieses Verfahren darlegen können, haben wir den folgenden Hilfssatz zu beweisen:

Hilfssatz. — Bezeichnet $f_2(x)$ den Rest der Division der beiden Polynome $f(x)$ und $f_1(x)$, deren erste Terme zum Coefficienten die Einheit haben, so sind die gemeinschaftlichen Wurzeln der beiden Congruenzen

$$f(x) \equiv 0 \quad , \quad f_1(x) \equiv 0 \ (mod.\ p)$$

dieselben, wie die gemeinschaftlichen Wurzeln von

$$f_1(x) \equiv 0 \quad , \quad f_2(x) \equiv 0 \ (mod.\ p) \ .$$

Ist Q der Quotient der Division von $f(x)$ durch $f_1(x)$, so hat man

$$f(x) = f_1(x) \cdot Q + f_2(x) \ ,$$

und diese Identität lässt erkennen, dass, wenn $f_1(x)$ und gleichzeitig eins der beiden Polynome $f(x)$ und $f_2(x)$ durch p theilbar sind, auch das andere durch p theilbar sein muss; hieraus ergiebt sich der angegebene Satz.

Zusatz. — Die den beiden Congruenzen

$$f(x) \equiv 0 \quad , \quad f_1(x) \equiv 0 \ (mod.\ p)$$

gemeinschaftlichen Wurzeln gehören der Congruenz

$$\varphi(x) \equiv 0 \ (mod.\ p)$$

an, wenn $\varphi(x)$ den grössten gemeinschaftlichen Divisor der beiden Polynome $f(x)$ und $f_1(x)$ bezeichnet.

Anmerkung. — Man bestimmt diesen grössten gemeinschaftlichen Divisor auf die gewöhnliche Weise; nur hat man alle mit p multiplicirten Terme zu vernachlässigen. Ausserdem müssen alle Divisionen ausgeführt werden können, ohne dass man dadurch zu gebrochenen Coefficienten gelangt. Zu diesem Zwecke richtet man es auf die oben angegebene Weise so ein, dass jeder Rest

durch den Coefficienten seines ersten Terms theilbar ist und abstrahirt sodann von diesem gemeinschaftlichen Divisor. Man gelangt auch dadurch zum Ziele, dass man jeden Dividenden mit einem geeigneten Factor multiplicirt, oder einfach dadurch, dass man zum Coefficienten des ersten Terms jedes Dividenden ein solches Multiplum von p addirt, dass der erste Term des in Rede stehenden Dividenden nach dieser Addition durch den ersten Term des entsprechenden Divisors theilbar ist.

301. Wir stellen uns jetzt die Aufgabe, die Anzahl der Wurzeln der Congruenz

$$f(x) \equiv 0 \pmod{p} \tag{1}$$

zu bestimmen. Diese Wurzeln gehören sämmtlich der Congruenz

$$x^{p-1} - 1 \equiv 0 \pmod{p} \tag{2}$$

an; es genügt also, die Wurzeln zu suchen, welche den Congruenzen (1) und (2) gemeinschaftlich sind. Zu diesem Zwecke bestimmen wir in der eben dargelegten Weise den grössten gemeinschaftlichen Divisor von $f(x)$ und $x^{p-1}-1$. Ist ein solcher nicht vorhanden, so besitzt die vorgelegte Congruenz (1) keine Wurzel. Ergiebt sich aber ein grösster gemeinschaftlicher Divisor $\varphi(x)$ vom Grade μ, so hat die vorgelegte Congruenz μ Wurzeln; es sind dies die Wurzeln der Congruenz

$$\varphi(x) \equiv 0 \pmod{p},$$

welche in der That μ Wurzeln besitzt, da $\varphi(x)$ ein Divisor μ^{ten} Grades des Binoms $x^{p-1}-1$ ist.

Beispiel. — Es soll untersucht werden, wie viele Wurzeln die Congruenz

$$f(x) = x^5 - 3x^4 - 2x^3 - 2x^2 + x - 2 \equiv 0 \pmod{7}$$

besitzt. Bestimmt man auf die in No. 300 angegebene Art den grössten gemeinschaftlichen Divisor der Polynome x^6-1 und $f(x)$, so erhält man die beiden Reste

$$-3(x^4 + 2x^3 + 3x^2 - 2x + 3),$$
$$2(x^3 + 3x^2 - x - 3);$$

da der zweite derselben in den ersten aufgeht, so hat die vorgelegte Congruenz drei Wurzeln, welche auch der Congruenz dritten Grades

$$x^3 + 3x^2 - x - 3 \equiv 0 \pmod{7}$$

angehören.

Neuer Beweis des Wilson'schen Satzes.

302. Bezeichnet p eine Primzahl, so besitzt die Congruenz
$(x-1)(x-2)(x-3)\ldots(x-p+1)-(x^{p-1}-1)\equiv 0 \ (mod.\ p)$
die $p-1$ Wurzeln

$$1\ ,\ 2\ ,\ 3\ ,\ \ldots\ ,\ (p-1)\ ,$$

und da sie nur vom $(p-2)^{\text{ten}}$ Grade ist, so muss sie identisch sein. Drückt also S_1 die Summe der Zahlen $1, 2, \ldots, (p-1)$ aus, S_2 die Summe aller aus je zwei derselben zu bildenden Produkte, u. s. w., S_{p-1} das Produkt aller dieser Zahlen, so hat man

$$S_1\equiv 0\ ,\ S_2\equiv 0\ ,\ S_3\equiv 0\ ,\ \ldots\ ,\ S_{p-1}\equiv -1\ (mod.\ p)\ .$$

Die letzte dieser Congruenzen ist der Ausdruck des Wilson'schen Satzes.

Anmerkung. — Ordnet man die Gleichung

$$(x-1)(x-2)(x-3)\ldots(x-p+1)=0$$

nach abnehmenden Potenzen von x, so sind, wenn p eine Primzahl ist, alle Coefficienten, mit Ausnahme des ersten und letzten, Vielfache von p. Mit Rücksicht hierauf ergiebt sich aus den Newton'schen Formeln unmittelbar, dass die Summe der m^{ten} Potenzen der $p-1$ Wurzeln

$$1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ \ldots\ ,\ (p-1)$$

durch p theilbar ist, wofern nicht m ein Multiplum von $p-1$ ist.

Zweites Kapitel.

Potenzreste und binomische Congruenzen.

Zahlen, welche in Beziehung auf einen gegebenen Modul zu einem gegebenen Exponenten gehören.

303. Wir betrachten die unendliche Reihe

$$(1).\qquad 1\ ,\ a\ ,\ a^2\ ,\ a^3\ ,\ \ldots\ ,\ a^n\ ,\ \ldots$$

der Potenzen einer Zahl a, welche prim zum Modul M ist. Da diese Reihe eine unbegrenzte Anzahl von Termen enthält, und es nur eine begrenzte Anzahl $\varphi(M)$ verschiedener Reste giebt, so müssen in (1) zwei Potenzen a^ν und $a^{n+\nu}$ vorkommen, welche nach dem Modul M congruent sind. Man kann die Congruenz

$$(2).\qquad a^{n+\nu} \equiv a^\nu\ (mod.\ M)$$

durch die Zahl a^ν, welche prim zum Modul ist, dividiren und erhält

$$(3).\qquad a^n \equiv 1\ (mod.\ M)\ .$$

Wenn umgekehrt die Congruenz (3) stattfindet, so besteht auch die Congruenz (2) für jeden Werth des Exponenten ν.

Ist also n die kleinste Zahl, für welche die Congruenz (3) gilt, so bilden die Reste der Reihe (1) eine periodische Reihe, deren Periode n nach dem Modul M incongruente Terme umfasst, nämlich die Reste der Potenzen

$$1\ ,\ a\ ,\ a^2\ ,\ \ldots\ ,\ a^{n-1}\ .$$

Die von Eins verschiedenen Terme der Reihe (1), welche den Rest 1 liefern, sind danach

$$a^n\ ,\ a^{2n}\ ,\ a^{3n}\ ,\ \ldots\ ;$$

nun hat man nach dem verallgemeinerten Fermat'schen Satze

$$a^{\varphi(M)} \equiv 1\ (mod.\ M)\ ,$$

folglich ist $\varphi(M)$ ein Vielfaches von n. Bezeichnet n die kleinste

positive Zahl, für welche $a^n \equiv 1 \pmod{M}$ ist, so sagt man, die Zahl a gehöre zum Exponenten n in Beziehung auf den Modul M. Mit Rücksicht hierauf lässt sich das Ergebniss der vorhergehenden Betrachtung folgendermassen aussprechen:

Lehrsatz. — Der Exponent, zu welchem irgend eine Zahl, die prim zum Modul M ist, in Beziehung auf diesen Modul gehört, ist ein Divisor von $\varphi(M)$.

304. Man kann zu diesem Resultate noch auf einem andern Wege gelangen, welcher den Fermat'schen Satz nicht voraussetzt und sogar zu einem neuen Beweise dieses Satzes führt.

Wenn a irgend eine ganze Zahl bedeutet, die prim zum Modul M ist, so liefert, wie wir uns überzeugt haben, die Reihe

$$(1). \qquad 1\ ,\ a\ ,\ a^2\ ,\ a^3\ ,\ \ldots\ ,\ a^n\ ,\ \ldots$$

eine gewisse Anzahl n verschiedener Reste, nämlich die Reste der Potenzen

$$(2) \qquad 1\ ,\ a\ ,\ a^2\ ,\ a^3\ ,\ \ldots\ ,\ a^{n-1}\ ,$$

und n ist die kleinste Zahl, für welche man

$$(3). \qquad a^n \equiv 1 \pmod{M}$$

hat.

Wenn die Reihe der Reste der Zahlen (2) alle Zahlen enthält, welche prim zu M und nicht grösser als M sind, so ist

$$\varphi(M) = n\ ;$$

im entgegengesetzten Falle sei b eine der Zahlen, die zu M prim, aber nach diesem Modul keinem Term der Reihe (2) congruent sind. Werden die Terme dieser Reihe mit b multiplicirt, so erhält man eine zweite Reihe

$$(4). \qquad b\ ,\ ba\ ,\ ba^2\ ,\ \ldots\ ,\ ba^{n-1}\ ,$$

deren Terme sämmtlich von einander verschieden sind; denn hätte man

$$ba^\mu \equiv ba^\nu \pmod{M}\ ,$$

so würde sich der Voraussetzung zuwider

$$a^\mu \equiv a^\nu \pmod{M}$$

ergeben. Ferner sind die Terme der Reihe (4) nach dem Modul M auch den Termen der Reihe (2) incongruent; denn wäre

$$ba^\mu \equiv a^\nu \pmod{M}\ ,$$

so müsste

$$b \equiv a^{\nu-\mu} \text{ oder } \equiv a^{n+\nu-\mu} \pmod{M}$$

sein, was gleichfalls der Voraussetzung widerspricht. Man erhält auf diese Weise entweder

$$\varphi(M) = 2n \text{ , oder } \varphi(M) > 2n .$$

Wenn $\varphi(M) > 2n$ ist, so sei c eine der Zahlen, welche prim zu M und nicht grösser als M sind, die sich nicht unter den Resten der Reihen (2) und (4) vorfindet. Multiplicirt man die Reihe (2) mit c, so erhält man eine neue Reihe

(5). $$c \text{ , } ca \text{ , } ca^2 \text{ , } ca^3 \text{ , } \ldots \text{ , } ca^{n-1} \text{ ,}$$

deren Terme nach dem Vorhergehenden denjenigen der Reihe (2) incongruent sind. Sie sind aber auch den Termen der Reihe (4) incongruent; wäre nämlich

$$ca^{\mu} \equiv ba^{\nu} \pmod{M} ,$$

so würde

$$c \equiv ba^{\nu-\mu} \text{ oder } \equiv ba^{n+\nu-\mu} \pmod{M} ,$$

also c im Gegensatz zu unserer Annahme unter den Resten der Reihe (4) enthalten sein müssen. Danach hat man entweder

$$\varphi(M) = 3n \text{ , oder } \varphi(M) > 3n .$$

In dieser Weise kann man fortfahren, bis die $\varphi(M)$ Zahlen, welche prim zu M und nicht grösser als M sind, völlig erschöpft sind, und man sieht, dass

$$\varphi(M) = mn$$

sein muss, wo m eine ganze Zahl ist; dies ist aber der in der vorigen Nummer bewiesene Satz.

Die Congruenz (3) zieht nothwendig

$$a^{mn} \equiv 1 \pmod{M} ,$$

oder

$$a^{\varphi(M)} \equiv 1 \pmod{M}$$

nach sich, und diese letzte Formel ist der Ausdruck des verallgemeinerten Fermat'schen Satzes.

Primitive Wurzeln.

305. Nach dem verallgemeinerten Fermat'schen Satze lässt die Congruenz

$$x^{\varphi(M)} \equiv 1 \pmod{M}$$

als Wurzeln die $\varphi(M)$ Zahlen zu, welche prim zu M und nicht grösser als M sind. Diejenigen dieser Zahlen, welche in Beziehung auf den Modul M zum Exponenten $\varphi(M)$ gehören, heissen

primitive Wurzeln der vorhergehenden Congruenz, oder einfach primitive Wurzeln der Zahl M.

Die Zahl a, welche prim zu M ist, wird demnach eine primitive Wurzel von M sein, wenn a^n für alle Werthe von n, die kleiner als $\varphi(M)$ sind, der Einheit nach dem Modul M incongruent ist. In diesem Falle bilden die Reste der Potenzen

$$1\ ,\ a\ ,\ a^2\ ,\ \ldots\ ,\ a^{\varphi(M)-1}$$

eine Reihe, welche alle Zahlen umfasst, die prim zu M und nicht grösser als M sind.

Es lässt sich nun zeigen, dass primitive Wurzeln nur in wenig ausgedehnten Fällen existiren.

Wir zerlegen den Modul M in seine Primfactoren; es ergebe sich

$$M = p^\nu q^\mu r^\lambda \ldots,$$

wo $p, q, r, \ldots$ ungleiche Primzahlen bezeichnen. Jede Zahl a, welche prim zu M ist, wird auch prim zu jedem der Factoren $p^\nu, q^\mu, r^\lambda, \ldots$ sein, und man erhält nach dem verallgemeinerten Fermat'schen Satze

$$a^{\varphi(p^\nu)} \equiv 1\ (mod.\ p^\nu)\ ,$$
$$a^{\varphi(q^\mu)} \equiv 1\ (mod.\ q^\mu)\ ,$$
$$a^{\varphi(r^\lambda)} \equiv 1\ (mod.\ r^\lambda)\ ,$$
$$\ldots\ldots\ldots\ldots$$

Bezeichnet S die kleinste der Zahlen, welche durch jede der folgenden theilbar sind:

$$\varphi(p^\nu) = p^{\nu-1}(p-1)\ ,$$
$$\varphi(q^\mu) = q^{\mu-1}(q-1)\ ,$$
$$\varphi(r^\lambda) = r^{\lambda-1}(r-1)\ ,$$
$$\ldots\ldots\ldots\ldots,$$

so hat man auch

$$a^S \equiv 1\ (\text{mod.}\ p^\nu)\ ,\ a^S \equiv 1\ (\text{mod.}\ q^\mu)\ ,\ a^S \equiv 1\ (\text{mod.}\ r^\lambda)\ ,\ \ldots.$$

Die Differenz $a^S - 1$ ist somit durch jede der Zahlen $p^\nu, q^\mu, r^\lambda, \ldots$ theilbar; sie muss daher durch das Produkt M dieser Zahlen theilbar sein, und man erhält

$$a^S \equiv 1\ (mod.\ M)\ .$$

Nun ist $\varphi(p^\nu)$ eine gerade Zahl, ausser wenn man $p = 2,\ \nu = 1$ hat. Ebenso ist $\varphi(q^\mu)$ gerade, ausser wenn $q = 2,\ \mu = 1$ ist, u. s. w. Wenn daher M mehr als einen ungeraden Primfactor

enthält, oder, wenn zwar nur ein ungerader Primfactor, aber eine höhere als die erste Potenz von 2 in M enthalten ist, so haben wenigstens zwei der Zahlen

$$\varphi(p^\nu)\ ,\ \varphi(q^\mu)\ ,\ \varphi(r^\lambda)\ ,\ \ldots$$

einen gemeinschaftlichen Divisor, und das kleinste gemeinschaftliche Vielfache dieser Zahlen ist folglich kleiner als ihr Produkt, d. h. es ist

$$S < \varphi(M)\ ;$$

dann ist aber die Zahl a, für welche man $a^S \equiv 1$ (*mod.* M) hat, keine primitive Wurzel von M.

Wir haben noch den Fall zu untersuchen, in welchem M keinen ungeraden Primfactor enthält; dann ist

$$M = 2^\nu\ ,\ \varphi(M) = 2^{\nu-1}\ ,$$

und wir behaupten, dass es keine primitiven Wurzeln giebt, wenn $\nu > 2$ ist.

Jede ungerade Zahl kann nämlich durch die Formel

$$a = \pm 1 + 2^2 k$$

dargestellt werden; daraus ergiebt sich leicht:

$$\begin{aligned} a^2 &= 1 + 2^3 k_1\ , \\ a^{2^2} &= 1 + 2^4 k_2\ , \\ a^{2^3} &= 1 + 2^5 k_3\ , \\ &\ldots\ldots\ldots\ , \\ a^{2^{\nu-2}} &= 1 + 2^\nu k_{\nu-2}\ , \end{aligned}$$

worin k_1, k_2, ..., $k_{\nu-2}$ ganze Zahlen bedeuten. Die letzte dieser Formeln lässt sich, wenn $\nu > 2$ ist, in folgender Weise schreiben:

$$a^{\frac{1}{2}\varphi(M)} \equiv 1\ (mod.\ M)\ ;$$

a ist folglich keine primitive Wurzel.

Die vorstehende Betrachtung lehrt, dass es nur in den folgenden drei Fällen primitive Wurzeln geben kann:

1⁰. Wenn der Modul M eine ungerade Primzahl oder eine Potenz einer ungeraden Primzahl ist;

2⁰. Wenn der Modul M gleich dem Doppelten einer solchen Potenz ist;

3⁰. Wenn der Modul M gleich 4 ist.

Für $M = 4$ hat man $\varphi(M) = 2$, und der Definition der primitiven Wurzeln genügt offenbar die Zahl -1 oder 3. Der Fall,

in welchem $M = 2^\nu > 4$ ist, verdient besondere Beachtung, obwohl dann von eigentlichen primitiven Wurzeln nicht mehr die Rede ist.

Primitive Wurzeln einer ungeraden Primzahl.

306. Wenn der Modul M sich auf eine ungerade Primzahl p reducirt, so ist $\varphi(M) = p - 1$. In diesem Falle giebt es immer primitive Wurzeln, deren Anzahl sich leicht mittels des folgenden Satzes (Gauss, disquisitt. 52—54) bestimmen lässt:

Lehrsatz. — Ist p eine Primzahl, und bezeichnet n irgend einen Divisor von $p-1$, so giebt es genau $\varphi(n)$ Zahlen, welche zum Exponenten n gehören; das Symbol $\varphi(n)$ drückt aus, wie viele Zahlen prim zu n und nicht grösser als n sind.

Wir nehmen an, es gäbe eine in Beziehung auf den Modul p zum Exponenten n gehörende Zahl a. Dann sind die Reste der Potenzen

(1). $$1\ ,\ a\ ,\ a^2\ ,\ \ldots\ ,\ a^{n-1}$$

von einander verschieden, und jeder derselben ist eine Wurzel der Congruenz

(2). $$x^n - 1 \equiv 0\ (mod.\ p)\ ;$$

denn wenn e irgend eine der Zahlen

$$0\ ,\ 1\ ,\ 2\ ,\ \ldots\ ,\ n-1$$

ist, so zieht die Voraussetzung

$$a^n \equiv 1\ (mod.\ p)$$

die Congruenz

(3). $$a^{ne} \equiv 1\ (mod.\ p)\ ,\ \text{oder}\ (a^e)^n - 1 \equiv 0\ (mod.\ p)$$

nach sich. Nach dem Lehrsatze der No. 298 hat daher die Congruenz (2) keine anderen Wurzeln, als die Reste der in (1) enthaltenen Potenzen. Wenn es also, ausser a, Zahlen giebt, die zum Exponenten n gehören, so muss jede derselben nach dem Modul p einer Potenz a^e von a congruent sein.

Bezeichnet m den Exponenten, zu welchem a^e gehört, so muss der Congruenz (3) wegen n ein Vielfaches von m sein; ausserdem hat man

(4). $$(a^e)^m \equiv 1\ (\text{mod.}\ p)\ \text{oder}\ a^{me} \equiv 1\ (\text{mod.}\ p)\ ,$$

und da a zum Exponenten n gehört, so muss me ein Vielfaches von n sein. Wenn daher e prim zu n ist, so muss m ein Viel-

faches von n sein; es ist dann jede der beiden Zahlen m und n durch die andere theilbar, d. h. es ist $m = n$. a^e gehört also zum Exponenten n, wenn e prim zu n ist. Haben aber die Zahlen e und n einen gemeinschaftlichen Divisor $\vartheta > 1$, so lässt sich die Congruenz

$$\left(a^{\frac{e}{\vartheta}}\right)^n \equiv 1 \ (mod.\ p)$$

in folgender Weise schreiben

$$(a^e)^{\frac{n}{\vartheta}} \equiv 1 \ (mod.\ p)\,,$$

und daraus geht hervor, dass a^e zu einem Exponenten gehört, der kleiner als n ist.

Wir erhalten somit das folgende Resultat:

Die Existenz einer Zahl vorausgesetzt, die in Beziehung auf den Modul p zum Exponenten n gehört, giebt es genau $\varphi(n)$ zu diesem Exponenten gehörende Zahlen.

Nun ist bekanntlich der Exponent, zu welchem irgend eine der Zahlen

$$(5). \qquad 1\ ,\ 2\ ,\ 3\ ,\ \ldots\ ,\ p-1$$

in Beziehung auf den Modul p gehört, gleich einem der Divisoren

$$(6). \qquad d\ ,\ d'\ ,\ d''\ ,\ d'''\ ,\ \ldots$$

der Zahl $p-1$. Bedient man sich des Symbols $\psi(d)$, um auszudrücken, wie viele Zahlen der Reihe (5) zum Exponenten d gehören, so hat man nach dem Vorhergehenden entweder

$$\psi(d) = \varphi(d)\ ,\ \text{oder}\ \psi(d) = 0\,.$$

In gleicher Weise sollen $\psi(d')$, $\psi(d'')$, ... ausdrücken, wie viele Zahlen der Reihe (5) beziehungsweise zu den Exponenten d', d'', ... gehören. Die Einheit ist in der Reihe der Divisoren (6) enthalten, und da 1 offenbar die einzige Zahl ist, welche zum Exponenten 1 gehört, so hat man

$$\psi(1) = 1\,.$$

Da endlich die Reihe (5) aus $p-1$ Termen besteht, und da jeder derselben zu einem der in (6) enthaltenen Exponenten gehört, so hat man die Identität

$$\psi(d) + \psi(d') + \psi(d'') + \cdots = p-1\,.$$

Es ist aber auch (No. 286)

$$\varphi(d) + \varphi(d') + \varphi(d'') + \cdots = p-1\,,$$

folglich

$$(7). \quad \psi(d)+\psi(d')+\psi(d'')+\cdots=\varphi(d)+\varphi(d')+\varphi(d'')+\cdots.$$

Wie wir oben gesehen haben, sind die von Null verschiedenen Terme des ersten Gliedes dieser Formel beziehungsweise gleich den Termen, welche im zweiten Gliede dieselben Plätze einnehmen. Man kann diese gleichen Terme auf beiden Seiten unterdrücken. Dadurch reducirt sich das erste Glied von (7) auf Null; dasselbe muss daher mit dem zweiten Gliede der Fall sein, d. h. man hat für jeden Divisor d

$$\psi(d) = \varphi(d).$$

Zusatz. — Es giebt $\varphi(p-1)$ Zahlen, welche in Beziehung auf den Primzahl-Modul p zum Exponenten $p-1$ gehören, oder mit andern Worten: es giebt $\varphi(p-1)$ primitive Wurzeln der Primzahl p.

Anmerkung. — Die Zahlen, welche in Beziehung auf den Primzahl-Modul p zu irgend einem Divisor n von $p-1$ gehören, nennt man auch wohl primitive Wurzeln der Congruenz $x^n \equiv 1 \pmod{p}$. Diese Congruenz hat nach dem Vorhergehenden n Wurzeln und darunter $\varphi(n)$ primitive.

307. Wir wollen hier noch einen sehr wichtigen Satz herleiten, den wir später anwenden werden.

Lehrsatz. — Wenn zwei Zahlen a und b in Beziehung auf einen Primzahlmodul p zu zwei Exponenten m und n gehören, die prim zu einander sind, so gehört das Produkt ab zum Exponenten mn.

Es sei s ein solcher Exponent, dass

$$(ab)^s = a^s b^s \equiv 1 \pmod{p}$$

ist. Wird diese Congruenz auf die m^{te} Potenz erhoben, so ergiebt sich

$$a^{ms} b^{ms} \equiv 1 \pmod{p}.$$

Da aber a zum Exponenten m gehört, so ist

$$a^{ms} \equiv 1 \pmod{p},$$

folglich auch

$$b^{ms} \equiv 1 \pmod{p},$$

oder ms ist ein Multiplum des Exponenten n, zu welchem b gehört. Ausserdem sind m und n relative Primzahlen; s muss daher ein Vielfaches von n sein. Ebenso könnte man zeigen, dass s ein Vielfaches von m ist. Daraus folgt, dass s durch das Produkt mn theilbar ist. Nun hat man der Voraussetzung nach

$$a^m \equiv 1 \quad , \quad b^n \equiv 1 \pmod{p} ,$$

also

$$a^{mn} \, b^{mn} = (ab)^{mn} \equiv 1 \pmod{p} ;$$

mithin ist das Produkt mn der Exponent, zu welchem ab gehört.

Zusatz I. — Wenn die Zahlen $a, b, c, \ldots$ in Beziehung auf den Modul p beziehungsweise zu den Exponenten $m, n, r, \ldots$ gehören, von denen je zwei prim zu einander sind, so gehört das Produkt $abc \ldots$ zum Exponenten $mnr \ldots$.

Zusatz II. — Es sei die Zahl $p-1$ gleich dem Produkte $2^\varrho q^\lambda r^\mu \ldots$, wo $q, r, \ldots$ von einander verschiedene ungerade Primzahlen sind. Bezeichnen dann $a, b, c, \ldots$ Zahlen, welche beziehungsweise zu den Exponenten $2^\varrho, q^\lambda, r^\mu, \ldots$ gehören, so gehört das Produkt $abc \ldots$ oder sein Rest zum Exponenten $p-1$ und ist folglich primitive Wurzel von p.

Andere Herleitung der vorhergehenden Resultate.

308. Die Sätze, die wir für Primzahlmoduln entwickelt haben, können, wie wir jetzt zeigen wollen, noch durch eine andere Methode bewiesen werden, welche mit der im V^ten Kapitel des I^ten Theils bei der Betrachtung der Wurzeln der binomischen Gleichungen in Anwendung gebrachten identisch ist. Wir halten es für nützlich, den Zusammenhang hervortreten zu lassen, der zwischen beiden Theorien besteht.

Lehrsatz I. — Die zweien binomischen Congruenzen

$$x^m \equiv 1 \pmod{p} \quad , \quad x^n \equiv 1 \pmod{p} ,$$

deren Modul p eine Primzahl ist, gemeinschaftlichen Wurzeln sind auch Wurzeln der Congruenz

$$x^\vartheta \equiv 1 \pmod{p} ,$$

worin ϑ der grösste gemeinschaftliche Divisor von m und n ist.

$x^\vartheta - 1$ ist nämlich der grösste gemeinschaftliche Divisor von $x^m - 1$ und $x^n - 1$. Unser Satz ist daher eine Folge des in No. 300 bewiesenen Zusatzes.

Umgekehrt muss offenbar jede Wurzel von $x^\vartheta \equiv 1 \pmod{p}$ auch den beiden vorgelegten Congruenzen genügen.

Zusatz. — Bezeichnet ϑ den grössten gemeinschaftlichen Divisor der Zahlen m und $p-1$, so hat die Congruenz

$$x^m \equiv 1 \ (mod.\ p)$$

ϑ Wurzeln, welche der Congruenz

$$x^\vartheta \equiv 1 \ (mod.\ p)$$

angehören.

Die Wurzeln der vorgelegten Congruenz sind nämlich auch Wurzeln von

$$x^{p-1} - 1 \equiv 0 \ (mod.\ p) .$$

Ausserdem hat die Congruenz

$$x^\vartheta - 1 \equiv 0$$

ϑ Wurzeln (No. 299), da ihr erstes Glied ein Divisor von $x^{p-1} - 1$ ist; die vorgelegte Congruenz besitzt daher selbst ϑ Wurzeln.

Wenn m prim zu $p-1$ ist, so hat man $\vartheta = 1$. In diesem Falle besitzt die Congruenz $x^m \equiv 1 \ (mod.\ p)$ keine Wurzel ausser der Einheit.

Man kann sich daher bei der Untersuchung der binomischen Congruenzen von der Form

$$x^m \equiv 1 \ (mod.\ p)$$

auf diejenigen beschränken, deren Grad m ein Divisor von $p-1$ ist.

Lehrsatz II. — Bezeichnet a irgend eine Wurzel der Congruenz

$$x^m \equiv 1 \ (mod.\ p) ,$$

deren Modul eine Primzahl und deren Grad m ein Divisor von $p-1$ ist, so ist jede Potenz von a oder ihr kleinster Rest gleichfalls eine Wurzel.

Die Congruenz

$$a^m \equiv 1 \ (mod.\ p)$$

zieht nämlich

$$a^{mk} \equiv 1 \text{ oder } (a^k)^m \equiv 1$$

nach sich, und wenn b den kleinsten Rest von a^k nach dem Modul p bezeichnet, so hat man

$$a^k \equiv b \quad , \text{ folglich } b^m \equiv 1 ;$$

daher sind alle Terme der Reihe

$$a \ , \ a^2 \ , \ a^3 \ , \ \ldots$$

oder ihre kleinsten Reste Wurzeln derselben Congruenz. Nun ist der Formel $a^m \equiv 1$ wegen

$$a^{m+1} \equiv a \quad , \quad a^{m+2} \equiv a^2 \quad , \quad \ldots .$$

Die vorhergehende Reihe enthält also höchstens m Terme, welche verschiedene Reste geben, und diese Reste kehren periodisch wieder. Wenn die m ersten Terme

$$a \; , \; a^2 \; , \; a^3 \; , \; \ldots \; , \; a^{m-1} \; , \; a^m \text{ oder } 1$$

nach dem Modul p incongruent sind, so sind ihre Reste die m Wurzeln der vorgelegten Congruenz. Im entgegengesetzten Falle, wenn etwa

$$a^{n+n'} \equiv a^{n'} \pmod{p}$$

ist, so kann man, da a prim zu p ist, durch $a^{n'}$ dividiren und erhält

$$a^n \equiv 1 \pmod{p} .$$

a ist folglich Wurzel einer binomischen Congruenz

$$x^n \equiv 1 \pmod{p} ,$$

deren Grad n kleiner als m ist. Die vorstehende Betrachtung liefert folgenden Satz:

Lehrsatz III. — Wenn a eine Wurzel der Congruenz $x^m \equiv 1 \pmod{p}$ ist, welche keiner Congruenz niedrigeren Grades $x^n \equiv 1 \pmod{p}$ angehört, so sind die m Wurzeln der vorgelegten Congruenz die Reste der m Potenzen

$$a \; , \; a^2 \; , \; a^3 \; , \; \ldots \; , \; a^{m-1} \; , \; a^m .$$

Die Analogie der Theorie, die wir hier darlegen, mit derjenigen der binomischen Gleichungen führt uns naturgemäss dazu, den Namen primitive Wurzeln einer binomischen Congruenz

$$x^m \equiv 1 \pmod{p} ,$$

deren Grad m in $p-1$ aufgeht, denjenigen Wurzeln dieser Congruenz beizulegen, welche keiner Congruenz von derselben Form und von einem niedrigeren Grade angehören. Wie im Falle binomischer Gleichungen besitzt jede primitive Wurzel die Eigenschaft, alle übrigen Wurzeln durch ihre verschiedenen Potenzen zu geben.

Man beachte, dass jede nicht primitive Wurzel der Congruenz $x^m \equiv 1 \pmod{p}$, da sie einer Congruenz derselben Form und niedrigeren Grades angehört, auch eine dritte Congruenz derselben Form befriedigt, deren Grad in den der vorgelegten aufgeht.

309. Die Existenz der primitiven Wurzeln lässt sich jetzt in folgender Weise darthun:

Wir betrachten die Congruenz

$$(1). \qquad x^m \equiv 1 \pmod{p} ,$$

und setzen zunächst voraus, es sei

$$m = q^\mu ,$$

d. h. m enthalte nur einen Primfactor q. Jede nicht primitive Wurzel von

(2). $$x^{q^\mu} \equiv 1 \ (mod.\ p)$$

gehört einer Congruenz

$$x^\vartheta \equiv 1 \ (mod.\ p)$$

an, deren Grad ϑ ein Divisor von q^μ und sogar von $q^{\mu-1}$ ist; folglich genügt eine solche Wurzel auch der Congruenz

(3). $$x^{q^{\mu-1}} \equiv 1 \ (mod.\ p).$$

Ausserdem sind die Wurzeln von (3) auch Wurzeln von (2); ihre Anzahl ist $q^{\mu-1}$, und die vorgelegte Congruenz besitzt somit

$$q^\mu - q^{\mu-1} = q^\mu \left(1 - \frac{1}{q}\right)$$

primitive Wurzeln.

Es sei jetzt allgemein

$$m = q^\mu r^\nu \ldots s^\lambda ,$$

wo $q, r, \ldots, s$ ungleiche Primfactoren bezeichnen. Wir betrachten die Congruenzen

(4). $$x^{q^\mu} \equiv 1 \ (mod.\ p) \ , \ x^{r^\nu} \equiv 1 \ (mod.\ p) \ , \ \ldots \ , \ x^{s^\lambda} \equiv 1 \ (mod.\ p),$$

und nehmen an, a sei eine primitive Wurzel der ersten, b der zweiten, u. s. w., l der letzten Congruenz. Dann lehrt der in No. 307 bewiesene Satz, dass der Rest des Produktes

$$ab \ldots l$$

eine primitive Wurzel der vorgelegten Congruenz

(5). $$x^{q^\mu r^\nu \ldots s^\lambda} \equiv 1 \ (mod.\ p)$$

ist. Man kann dies aber auch auf folgende Weise darthun: Zunächst ist es klar, dass das Produkt $a\,b \ldots l$ oder sein Rest eine Wurzel von (5) ist; denn man hat

$$a^{q^\mu} \equiv 1 \ , \ b^{r^\nu} \equiv 1 \ , \ \ldots \ , \ l^{s^\lambda} \equiv 1 \ (mod.\ p) ,$$

folglich auch

$$(a\,b \ldots l)^{q^\mu r^\nu \ldots s^\lambda} \equiv 1 \ (mod.\ p) .$$

Wäre dieses Produkt nun keine primitive Wurzel der vorgelegten Congruenz, so würde es eine Congruenz

$$x^\vartheta \equiv 1 \ (mod.\ p)$$

befriedigen, deren Grad ϑ in m aufgeht; es müsste also wenigstens ein Primfactor von m in ϑ weniger oft als in m eingehen. Dieser Primfactor sei q; dann geht ϑ in $q^{\mu-1} r^{\nu} \ldots s^{\lambda}$ auf, und folglich ist $a\, b \ldots l$ eine Wurzel der Congruenz

$$x^{q^{\mu-1} r^{\nu} \ldots s^{\lambda}} \equiv 1 \pmod{p} ;$$

man hat daher

$$(a\, b \ldots l)^{q^{\mu-1} r^{\nu} \ldots s^{\lambda}} \equiv 1 \pmod{p} .$$

Es ist aber auch

$$(b \ldots l)^{q^{\mu-1} r^{\nu} \ldots s^{\lambda}} \equiv 1 \pmod{p} ,$$

und durch Division ergiebt sich aus den beiden letzten Congruenzen

$$a^{q^{\mu-1} r^{\nu} \ldots s^{\lambda}} \equiv 1 \pmod{p} .$$

Wie man sieht, ist a eine Wurzel der Congruenzen

$$x^{q^{\mu-1} r^{\nu} \ldots s^{\lambda}} \equiv 1 \text{ und } x^{q^{\mu}} \equiv 1 \pmod{p} ,$$

und da die Grade derselben den grössten gemeinschaftlichen Divisor $q^{\mu-1}$ haben, so muss a auch der Congruenz

$$x^{q^{\mu-1}} \equiv 1 \pmod{p}$$

genügen; a ist also nicht, wie wir vorausgesetzt haben, eine primitive Wurzel von $x^{q^{\mu}} \equiv 1 \pmod{p}$.

Wenn demnach a eine primitive Wurzel der ersten, b der zweiten, u. s. w., l der letzten der Congruenzen (4) bezeichnet, so ist das Produkt $a\, b \ldots l$ oder sein Rest eine primitive Wurzel der vorgelegten Congruenz (5). Ausserdem lässt sich mittels des in No. 104 bei der Betrachtung der binomischen Gleichung angewandten Schlussverfahrens darthun, dass alle Wurzeln von (5), sowohl die primitiven, als auch die nicht primitiven, durch die Formel

$$a\, b \ldots l$$

dargestellt werden, in welcher für $a, b, \ldots, l$ beziehungsweise alle Wurzeln der ersten, der zweiten, ..., der letzten der Congruenzen (4) zu nehmen sind, und dass diese Formel alle primitiven Wurzeln liefert, wenn man für $a, b, \ldots, l$ die verschiedenen primitiven Wurzeln derjenigen Congruenzen nimmt, denen sie angehören. Da es $q^{\mu}\left(1 - \frac{1}{q}\right)$ primitive Wurzeln a, $r^{\nu}\left(1 - \frac{1}{r}\right)$ primitive Wurzeln $b, \ldots, s^{\lambda}\left(1 - \frac{1}{s}\right)$ primitive Wurzeln l giebt, so besitzt die vorgelegte Congruenz

$$m\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots\left(1-\frac{1}{s}\right)=\varphi(m)$$

primitive Wurzeln.

Satz über die Reste von Potenzen, deren Grad ein Divisor von $p-1$ ist.

310. Lehrsatz. — Der Modul p sei eine Primzahl und ϑ ein Divisor von $p-1$; ferner bezeichnen x_1 und ξ zwei zwischen 0 und p enthaltene Zahlen; hat man dann

$$x_1^\vartheta \equiv \xi \pmod{p},$$

so ist auch

$$\xi^{\frac{p-1}{\vartheta}} \equiv 1 \pmod{p},$$

und wenn umgekehrt

$$\xi^{\frac{p-1}{\vartheta}} \equiv 1 \pmod{p}$$

ist, so besitzt die Congruenz

$$x^\vartheta \equiv \xi \pmod{p}$$

ϑ Wurzeln.

Der erste Theil des Satzes leuchtet unmittelbar ein; erhebt man nämlich beide Glieder der Congruenz

$$x_1^\vartheta \equiv \xi \pmod{p}$$

auf die $\left(\frac{p-1}{\vartheta}\right)^{\text{te}}$ Potenz, so ergiebt sich

$$x_1^{p-1} \equiv \xi^{\frac{p-1}{\vartheta}} \pmod{p},$$

oder, des Fermat'schen Satzes wegen,

$$\xi^{\frac{p-1}{\vartheta}} \equiv 1 \pmod{p}.$$

Umgekehrt sei $\xi^{\frac{p-1}{\vartheta}} \equiv 1$, oder

$$\xi^{\frac{p-1}{\vartheta}} - 1 = pQ.$$

Wird jedes Glied dieser Gleichung von $x^{p-1}-1$ subtrahirt, so folgt

$$x^{p-1}-1-pQ = x^{p-1}-\xi^{\frac{p-1}{\vartheta}} = (x^\vartheta)^{\frac{p-1}{\vartheta}} - \xi^{\frac{p-1}{\vartheta}}.$$

Das zweite Glied dieser Gleichung ist durch $x^\vartheta - \xi$ theilbar; dasselbe muss daher mit $x^{p-1}-1-pQ$ der Fall sein; folglich hat die Congruenz

$$x^\vartheta - \xi \equiv 0 \pmod{p}$$

nach dem in No. 299 bewiesenen Satze ϑ Wurzeln.

Zusatz. — Wenn p eine Primzahl ist, und wenn sich durch Zerlegung von $p-1$ in seine Primfactoren

$$p-1 = 2^{\varrho} q^{\mu} r^{\nu} \dots s^{\lambda}$$

ergiebt, so sind die nicht primitiven Wurzeln der Congruenz

$$x^{p-1} - 1 \equiv 0 \ (mod. \ p),$$

welche Wurzeln wenigstens einer der Congruenzen

$$x^{\frac{p-1}{2}} \equiv 1 \,,\; x^{\frac{p-1}{q}} \equiv 1 \,,\; x^{\frac{p-1}{r}} \equiv 1 \,,\; \dots ,\; x^{\frac{p-1}{s}} \equiv 1$$

angehören, Reste von Quadraten, oder von q^{ten} Potenzen, oder von r^{ten} Potenzen, u. s. w., oder von s^{ten} Potenzen. Umgekehrt ist jeder Rest eines Quadrats, oder einer q^{ten} Potenz, oder u. s. w. eine Wurzel einer der letzten Congruenzen und nicht primitive Wurzel der Primzahl p.

Dieser Zusatz ergiebt sich unmittelbar aus dem vorhergehenden Satze. Man kann hinzufügen, dass die Hälfte der Zahlen

$$1 \,,\, 2 \,,\, 3 \,,\, \dots ,\, p-1$$

Quadrate (Reste von Quadraten), der q^{te} Theil q^{te} Potenzen, der r^{te} Theil r^{te} Potenzen, u. s. w., der s^{te} Theil s^{te} Potenzen sind. Betrachtet man allgemeiner nur diejenigen dieser Zahlen, welche gleichzeitig 2te, q^{te}, r^{te}, ... Potenzen sind, so ist der s^{te} Theil derselben auch s^{te} Potenzen. Die Zahlen, welche gleichzeitig Reste von Quadraten, von q^{ten}, r^{ten}, u. s. w. Potenzen sind, genügen nämlich den Congruenzen

$$x^{\frac{p-1}{2}} \equiv 1 \,,\; x^{\frac{p-1}{q}} \equiv 1 \,,\; x^{\frac{p-1}{r}} \equiv 1 \,,\; \dots \ (mod. \ p),$$

und sind folglich Wurzeln von

$$x^{\frac{p-1}{2qr\dots}} \equiv 1 \ (mod. \ p);$$

ihre Anzahl ist daher $\frac{p-1}{2qr\dots}$. Die Anzahl derjenigen dieser Wurzeln, welche auch noch s^{te} Potenzen sind, ist $\frac{p-1}{2qr\dots s}$, mithin der s^{te} Theil der ersteren Zahl.

311. Die Congruenz

$$(1). \qquad x^{p-1} - 1 \equiv 0 \ (mod. \ p)$$

kann auf die Form

$$\left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right) \equiv 0 \ (mod. \ p)$$

gebracht werden, und jede der beiden Congruenzen

$$(2). \qquad x^{\frac{p-1}{2}} - 1 \equiv 0 \ (mod.\ p),$$

$$(3). \qquad x^{\frac{p-1}{2}} + 1 \equiv 0 \ (mod.\ p),$$

in die sie zerfällt, hat $\frac{p-1}{2}$ Wurzeln. Ausserdem ist nach dem Satze der No. 310 jede Wurzel der Congruenz (2) der Rest eines Quadrats oder ein quadratischer Rest. Dagegen kann keine Wurzel von (3) der Rest eines Quadrats sein; die Wurzeln dieser Congruenz (3) werden deshalb quadratische Nichtreste, oder einfach Nichtreste genannt.

Die Zahl a ist demnach ein quadratischer Rest oder Nichtrest für den Primzahlmodul p, jenachdem sie der Congruenz (2) oder der Congruenz (3) genügt, d. h. jenachdem die Division von $a^{\frac{p-1}{2}}$ durch p den Rest $+1$ oder den Rest -1 liefert. Legendre hat vorgeschlagen, diesen Rest durch das Symbol $\left(\frac{a}{p}\right)$ darzustellen, so dass man

$$\left(\frac{a}{p}\right) = +1$$

hat, wenn a ein quadratischer Rest, dagegen

$$\left(\frac{a}{p}\right) = -1,$$

wenn a ein Nichtrest ist.

Wenn p von der Form $4i+1$ ist, so sind die beiden Zahlen a und $-a$ offenbar gleichzeitig Reste oder Nichtreste. Hat aber p die Form $4i+3$, so ist eine der beiden Zahlen a und $-a$ ein Rest, die andere ein Nichtrest.

Sind die Zahlen a und b entweder beide Reste, oder beide Nichtreste, so hat man

$$a^{\frac{p-1}{2}} \equiv \pm 1, \quad b^{\frac{p-1}{2}} \equiv \pm 1, \quad \text{folglich } (ab)^{\frac{p-1}{2}} \equiv +1 \ (mod.\ p),$$

d. h. das Produkt ab ist ein Rest. Wenn dagegen eine der Zahlen a und b ein Rest, die andere ein Nichtrest ist, so hat man

$$a^{\frac{p-1}{2}} \equiv \pm 1, \quad b^{\frac{p-1}{2}} \equiv \mp 1, \quad \text{folglich } (ab)^{\frac{p-1}{2}} \equiv -1 \ (mod.\ p),$$

d. h. das Produkt ab ist ein Nichtrest.

Dieses Resultat lässt sich durch die Formel

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

ausdrücken, und es liegt auf der Hand, dass allgemein

$$\left(\frac{abcd\ldots}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\left(\frac{d}{p}\right)\cdots$$

ist. Wir werden später einen sehr schönen Satz von Legendre kennen lernen, welcher es ermöglicht, den Werth der Ausdrücke $\left(\frac{a}{p}\right)$ mit Leichtigkeit zu bestimmen.

Aufsuchung der primitiven Wurzeln einer Primzahl.

312. Der in No. 310 hergeleitete Satz liefert ein Mittel, die primitiven Wurzeln einer Primzahl p zu bestimmen.

Es seien $2, q, r, \ldots, s$ die ungleichen Primfactoren von $p-1$; werden dann aus der Reihe der $p-1$ Zahlen

$$1, 2, 3, 4, \ldots, p-1$$

alle Reste von 2ten, q^{ten}, r^{ten}, ..., s^{ten} Potenzen entfernt, so bleiben nur die primitiven Wurzeln von p zurück.

Durch Beseitigung der Quadrate schliesst man die Hälfte der Zahlen aus; durch Wegschaffung der q^{ten} Potenzen entfernt man den q^{ten} Theil der übrig gebliebenen Zahlen, u. s. w. Wir wollen z. B. die primitiven Wurzeln von 31 bestimmen. Zu diesem Zwecke schreiben wir die 30 Zahlen

$$(1). \quad \begin{cases} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, \\ 11, & 12, & 13, & 14, & 15, & 16, & 17, & 18, & 19, & 20, \\ 21, & 22, & 23, & 24, & 25, & 26, & 27, & 28, & 29, & 30 \end{cases}$$

auf. Da die Primfactoren von 30 2, 3 und 5 sind, so haben wir nur die Reste der zweiten, dritten und 5ten Potenzen aus der Reihe (1) zu entfernen.

Um die Quadrate auszuschliessen, erheben wir die Zahlen (1) auf die zweite Potenz. Die Quadrate der fünfzehn ersten Zahlen sind

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225;$$

sie haben die Reste

$$(2). \quad 1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8.$$

Die Quadrate der fünfzehn letzten Zahlen der Reihe (1) würden dieselben Reste liefern, da

$$(31-h)^2 \equiv h^2 \; (mod.\, 31)$$

ist. Lässt man die Zahlen (2) aus der Reihe (1) fort, so bleiben die fünfzehn Zahlen

(3). 3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30

zurück; es sind jetzt noch die 3ten und die 5ten Potenzen aus (3) fortzuschaffen. Jede schon unterdrückte Zahl (2) genügt der Congruenz

$$x^{15} \equiv 1 \; (mod.\, 31);$$

ihre dritte und ihre fünfte Potenz genügen dieser Congruenz gleichfalls, befinden sich also unter den bereits ausgeschiedenen Zahlen. Danach sind die Zahlen der Reihe (3), die noch beseitigt werden müssen, Reste von dritten und von fünften Potenzen ebenderselben Zahlen (3). Um die Reste der dritten Potenzen der Zahlen (3) zu erhalten, genügt es, die ersten Potenzen mit den quadratischen Resten zu multipliciren, welche die Reihe (2) kennen lehrt, und welche folgende sind:

9, 5, 28, 20, 14, 8, 10, 7, 19, 2, 18, 25, 16, 4, 1.

Man erhält auf diese Weise die folgenden kubischen Reste:

27, 30, 308, 240, 182, 120, 170, 147, 418, 46, 432, 650, 432, 116, 30;

ihre kleinsten Reste sind

(4). 27, 30, 29, 23, 27, 27, 15, 23, 15, 15, 29, 30, 29, 23, 30.

Wie wir im Voraus wussten, sind darunter nur fünf verschiedene, nämlich

(5). 15, 23, 27, 29, 30.

Werden diese aus der Reihe (3) fortgelassen, so bleiben nur noch die zehn Zahlen

(6). 3, 6, 11, 12, 13, 17, 21, 22, 24, 26

zurück. Es handelt sich jetzt darum, aus (6) die Zahlen zu entfernen, welche Reste von fünften Potenzen sind. Jede der schon ausgeschiedenen Zahlen genügt einer der Congruenzen

$$x^{15} \equiv 1 \; (mod.\, 31) \quad , \quad x^{10} \equiv 1 \; (mod.\, 31) \cdot$$

Dasselbe ist daher mit ihrer fünften Potenz der Fall, welche folglich sich unter den ausgeschiedenen Zahlen bereits vorfindet: eine

Zahl der Reihe (6) kann mithin die fünfte Potenz von keiner Zahl sein, die nicht in derselben Reihe (6) vorkommt. Um nun die Reste der fünften Potenzen der Zahlen (6) zu erhalten, genügt es, die schon gebildeten kubischen Reste mit den entsprechenden quadratischen Resten zu multipliciren, und die kleinsten Reste der so erhaltenen Produkte zu nehmen. Die kubischen Reste sind

$$27 , 30 , 29 , 23 , 27 , 15 , 23 , 15 , 29 , 30 ,$$

die quadratischen

$$9 , 5 , 28 , 20 , 14 , 10 , 7 , 19 , 18 , 25 .$$

Daraus bildet man die Produkte

$$243 , 150 , 812 , 460 , 378 , 150 , 161 , 285 , 522 , 750 ,$$

als deren kleinste Reste sich

$$26 , 26 , 6 , 26 , 6 , 26 , 6 , 6 , 26 , 6$$

ergeben. In der Reihe (6) sind danach, wie wir übrigens im Voraus wussten, nur zwei fünfte Potenzen, nämlich

$$6 , 26$$

vorhanden. Werden dieselben aus der Reihe (6) fortgelassen, so bleiben nur die acht Zahlen

$$3 , 11 , 12 , 13 , 17 , 21 , 22 , 24$$

übrig, und diese sind die primitiven Wurzeln von 31.

313. Die Aufsuchung der primitiven Wurzeln stützt sich hauptsächlich auf den Versuch. Das im Vorhergehenden angegebene Verfahren ist für einen auch nur wenig beträchtlichen Modul nicht mehr durchzuführen; deshalb halten wir es für nützlich, eine andere, von Gauss herrührende Methode hier mitzutheilen, mittels welcher man eine primitive Wurzel ziemlich leicht ermitteln kann. Die übrigen primitiven Wurzeln ergeben sich dann auf eine in No. 306 angedeutete Weise, die wir später an einem Beispiel kennen lernen werden. Die Methode von Gauss besteht im Folgenden:

Man nimmt eine beliebige Zahl a aus der Reihe 2, 3, ..., $(p-1)$, z. B. 2, und bestimmt die Periode derselben, d. h. die Periode der Reste, welche die Potenzen

$$a , a^2 , a^3 , \ldots$$

liefern. Enthält diese Periode $p-1$ Terme, so ist a eine primitive Wurzel. Im entgegengesetzten Falle nimmt man eine in

der Periode von a nicht vorkommende Zahl b und bestimmt auch deren Periode. Besteht letztere aus $p-1$ Termen, so ist b eine primitive Wurzel. Wir nehmen aber an, dies sei nicht der Fall, und bezeichnen mit n den Exponenten, zu welchem a, mit m den Exponenten, zu welchem b gehört. Da die Reste der Potenzen von a alle Zahlen umfassen, welche zum Exponenten n, und auch alle Zahlen, welche zu einem in n aufgehenden Exponenten gehören, so kann m kein Divisor von n sein. Es ist aber möglich, dass m ein Vielfaches von n ist, und in diesem Falle bringt uns die Kenntniss von b unserem Ziele insofern näher, als wir jetzt eine Zahl kennen, welche zu einem höheren Exponenten als a gehört. Es sei nun m weder gleich $p-1$, noch gleich einem Vielfachen von n. Wir bezeichnen das kleinste gemeinschaftliche Vielfache von n und m mit s und zerlegen s in zwei Factoren n', m', welche prim zu einander sind und beziehungsweise in die Zahlen n, m aufgehen. Diese Zerlegung kann folgendermassen ausgeführt werden: Man zerlegt die Zahlen n und m in ihre Primfactoren; einer derselben, dessen γ^{te} Potenz in s eingehen soll, sei c. Wenn c^γ ein Divisor von n allein ist, so macht man ihn zu einem Bestandtheile von n'; wenn umgekehrt c^γ nur in m aufgeht, so führt man c^γ in m' ein; wenn endlich c^γ ein gemeinschaftlicher Divisor von m und n ist, so kann man c^γ ganz nach Belieben entweder in n', oder in m' einführen. Ebenso verfährt man mit den übrigen Primfactoren von s. Es ist dann $s = n'm'$ und zugleich $n = n'e$, $m = m'f$, wo e und f ganze Zahlen bedeuten. Dies vorausgesetzt, behaupten wir, dass die Zahl a^e in Beziehung auf den Modul p zum Exponenten n' gehört; die n'^{te} Potenz von a^e ist nämlich a^n und liefert folglich den Rest 1; ausserdem kann für einen Exponenten ν, der kleiner als n' ist, $(a^e)^\nu$ oder $a^{\nu e}$ nicht congruent 1 sein; denn νe ist kleiner als n, und a gehört der Voraussetzung nach zum Exponenten n. Ebenso zeigt man, dass b^f zum Exponenten m' gehört; daraus ergiebt sich (No. 307), dass das Produkt $a^e \cdot b^f$ oder sein Rest zum Exponenten $m'n' = s$ gehört.

Diese Methode führt in allen Fällen zu einer Zahl, welche zu einem höheren Exponenten als diejenige Zahl gehört, von der man ausging. Durch wiederholte Anwendung des dargelegten Verfahrens wird man also sicherlich einmal zu einer Zahl, die zum Exponenten $p-1$ gehört, d. h. zu einer primitiven Wurzel von

p gelangen. Meist treten auch noch besondere Umstände ein, welche eine Vereinfachung der Methode gestatten.

314. Erstes Beispiel. — Es soll eine primitive Wurzel der Primzahl 71 ermittelt werden.

Wir bilden zunächst die Periode der Zahl 2. Zu diesem Zwecke haben wir die Reihe der Potenzen von 2 zu berechnen. Jede derselben wird dadurch erhalten, dass man die vorhergehende Potenz mit 2 multiplicirt. Vor dieser Multiplication ist der Einfachheit wegen jeder Multiplicand durch seinen kleinsten positiven Rest zu ersetzen. Es ergiebt sich, dass die Periode von 2 aus den folgenden 35 Termen besteht:

$$(1). \quad \left\{\begin{array}{rrrrrrr} 2, & 4, & 8, & 16, & 32, & 64, & 57, \\ 43, & 15, & 30, & 60, & 49, & 27, & 54, \\ 37, & 3, & 6, & 12, & 24, & 48, & 25, \\ 50, & 29, & 58, & 45, & 19, & 38, & 5, \\ 10, & 20, & 40, & 9, & 18, & 36, & 1. \end{array}\right.$$

Die Zahl 2 ist also keine primitive Wurzel, sondern gehört zum Exponenten 35. Es lässt sich aber leicht einsehen, dass ihre Ergänzung zu 71, d. h. die Zahl 69, eine primitive Wurzel von 71 sein muss. Aus der Identität

$$69 = 71 - 2$$

folgt nämlich

$$\left.\begin{array}{l} 69^2 \equiv 2^2 \\ 69^3 \equiv -2^3 \end{array}\right\} (mod.\ 71),$$

und diese Relationen setzen uns in den Stand, die Restreihe der Potenzen von 69 aus der Reihe (1) herzuleiten. Dies geschieht dadurch, dass wir die Reste gerader Ordnung ungeändert lassen, jeden Rest ungerader Ordnung dagegen durch seine Ergänzung zu 71 ersetzen. In der Reihe der Reste, welche die Potenzen von 2 liefern, und deren erste Periode die Gesammtheit der Zahlen (1) ist, nimmt der Rest 1 den 35ten, 70ten, ... Platz ein; in der Periode von 69 wird dieser Rest daher erst auf dem 70ten Platze erscheinen, folglich ist 69 eine primitive Wurzel. Bilden wir die Periode von 69 in der angegebenen Weise, d. h. dadurch, dass wir die Periode von 2 zweimal schreiben und jeden Term ungerader Ordnung durch seine Ergänzung zu 71 ersetzen, so ergiebt sich

$$(2).\quad \begin{cases} 69\,, & 4\,, & 63\,, & 16\,, & 39\,, & 64\,, & 14\,, \\ 43\,, & 56\,, & 30\,, & 11\,, & 49\,, & 44\,, & 54\,, \\ 34\,, & 3\,, & 65\,, & 12\,, & 47\,, & 48\,, & 46\,, \\ 50\,, & 42\,, & 58\,, & 26\,, & 19\,, & 33\,, & 5\,, \\ 61\,, & 20\,, & 31\,, & 9\,, & 53\,, & 36\,, & 70\,, \\ 2\,, & 67\,, & 8\,, & 55\,, & 32\,, & 7\,, & 57\,, \\ 28\,, & 15\,, & 41\,, & 60\,, & 22\,, & 27\,, & 17\,, \\ 37\,, & 68\,, & 6\,, & 59\,, & 24\,, & 23\,, & 25\,, \\ 21\,, & 29\,, & 13\,, & 45\,, & 52\,, & 38\,, & 66\,, \\ 10\,, & 51\,, & 40\,, & 62\,, & 18\,, & 35\,, & 1\,, \end{cases}$$

und allgemein ist die k^{te} dieser Zahlen eine primitive Wurzel von 71, wenn k prim zu 70 ist. Danach hat 71 die 24 primitiven Wurzeln

$$\begin{array}{cccccccc} 69\,, & 63\,, & 56\,, & 11\,, & 44\,, & 65\,, & 47\,, & 42\,, \\ 33\,, & 61\,, & 31\,, & 53\,, & 67\,, & 55\,, & 7\,, & 28\,, \\ 22\,, & 68\,, & 59\,, & 21\,, & 13\,, & 52\,, & 62\,, & 35\,; \end{array}$$

die kleinste derselben ist 7.

315. Zweites Beispiel. — Es soll eine primitive Wurzel der Primzahl 73 ermittelt werden.

Wir bilden zunächst wieder die Periode der Zahl 2, die in diesem Falle nur die 9 Zahlen

$$2\,,\ 4\,,\ 8\,,\ 16\,,\ 32\,,\ 64\,,\ 55\,,\ 37\,,\ 1$$

enthält; die Zahl 2 gehört daher in Beziehung auf den Modul 73 zum Exponenten 9. Da 3 in der vorhergehenden Reihe nicht vorkommt, so bilden wir die Periode von 3. Es ergiebt sich

$$\begin{array}{cccccc} 3\,, & 9\,, & 27\,, & 8\,, & 24\,, & 72\,, \\ 70\,, & 64\,, & 46\,, & 65\,, & 49\,, & 1\,; \end{array}$$

3 gehört also zum Exponenten 12. Das kleinste gemeinschaftliche Vielfache von 9 und 12 ist 36; die in No. 307 auseinandergesetzte Methode wird folglich eine zum Exponenten 36 gehörende Zahl liefern. Dieser Exponent 36 ist das Produkt der Factoren 9 und 4, welche prim zu einander sind und beziehungsweise in 9 und 12 aufgehen; die Quotienten dieser Divisionen sind 1 und 3; mithin gehört die Zahl $2 \times 3^3 = 54$ zum Exponenten 36. Die Periode von 54 besteht aus den 36 Termen:

54 , 69 , 3 , 16 , 61 , 9 , 48 , 37 , 27 ,
71 , 38 , 8 , 67 , 41 , 24 , 55 , 50 , 72 ,
19 , 4 , 70 , 57 , 12 , 64 , 25 , 36 , 46 ,
2 , 35 , 65 , 6 , 32 , 49 , 18 , 23 , 1 ,

deren Berechnung durch Berücksichtigung der Relation

$$54^3 \equiv 3 \ (mod.\ 73) ,$$

aus welcher

$$54^k \equiv 3 \,.\, 54^{k-3} \ (mod.\ 73)$$

folgt, bedeutend vereinfacht wird. In der Periode von 54 ist die Zahl 5 nicht enthalten; 5^2 oder 25 kommt aber darin vor, und zwar nimmt 25 den 25ten Platz ein. Da nun 25 prim zu 72 ist, so gehört die Zahl 25 zum Exponenten 36, also die Zahl 5 zum Exponenten 36×2 oder 72; 5 ist daher eine primitive Wurzel von 73.

316. Wir lassen hier eine Tabelle folgen, in welcher die kleinste primitive Wurzel jeder Primzahl angegeben ist, die zwischen 3 und 1000 liegt. Alle Primzahlen, welche die primitive Wurzel 10 haben, sind mit dem Zeichen * versehen.

Primzahl	Prim. Wrzl.	Primzahl	Prim. Wrzl.	Primzahl	Prim. Wrzl.	Primzahl	Prim. Wrzl.
3	2	83	2	193 *	5	313 *	10
5	2	89	3	197	2	317	2
7	3	97 *	5	199	3	331	3
11	2	101	2	211	2	337 *	10
13	2	103	5	223 *	3	347	2
17 *	3	107	2	227	2	349	2
19 *	2	109 *	6	229 *	6	353	3
23 *	5	113 *	3	233 *	3	359	7
29 *	2	127	3	239	7	367 *	6
31	3	131 *	2	241	7	373	2
37	2	137	3	251	6	379 *	2
41	6	139	2	257 *	3	383 *	5
43	3	149 *	2	263 *	5	389 *	2
47 *	5	151	6	269 *	2	397	5
53	2	157	5	271	6	401	3
59 *	2	163	2	277	5	409	21
61 *	2	167 *	5	281	3	419 *	2
67	2	173	2	283	3	421	2
71	7	179 *	2	293	2	431	7
73	5	181 *	2	307	5	433 *	5
79	3	191	19	311	17	439	15

Primzahl	Prim. Wrzl.	Primzahl	Prim. Wrzl.	Primzahl	Prim. Wrzl.	Primzahl	Prim. Wrzl.
443	2	587	2	719	11	859	2
449	3	593 *	3	727 *	5	863 *	5
457	13	599	7	733	6	877	2
461 *	2	601	7	739	3	881	3
463	3	607	3	743 *	5	883	2
467	2	613	2	751	3	887 *	5
479	13	617	3	757	2	907	2
487 *	3	619 *	2	761	6	911	17
491 *	2	631	3	769	11	919	7
499 *	7	641	3	773	2	929	3
503 *	5	643	11	787	2	937 *	5
509 *	2	647 *	5	797	2	941 *	2
521	3	653	2	809	3	947	2
523	2	659 *	2	811 *	3	953 *	3
541 *	2	661	2	821 *	2	967	5
547	2	673	5	823 *	3	971 *	6
557	2	677	2	827	2	977 *	3
563	2	683	5	829	2	983 *	5
569	3	691	3	839	11	991	6
571 *	3	701 *	2	853	2	997	7
577 *	5	709 *	2	857 *	3		

Bei dieser Gelegenheit theilen wir noch die folgenden Bemerkungen mit:

1⁰. Wenn p von der Form $4k+1$ und a eine primitive Wurzel ist, so ist auch $-a$ eine primitive Wurzel.

2⁰. Wenn p von der Form $4k+3$ ist, so können a und $-a$ nicht gleichzeitig primitive Wurzeln sein.

Jede nicht primitive Wurzel von p genügt nämlich einer Congruenz

$$x^{\frac{p-1}{\vartheta}} \equiv 1 \pmod{p},$$

in welcher ϑ eine in $p-1$ aufgehende Primzahl ist. Hat man $p = 4k+1$, so ist $\frac{p-1}{\vartheta}$ eine gerade Zahl, und je zwei Wurzeln der vorhergehenden Congruenz sind einander entgegengesetzt gleich. Wenn zweitens $p = 4k+3$ ist, und a der Congruenz

$$x^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

genügt, so genügt $-a$ der Congruenz

$$x^{\frac{p-1}{2}} \equiv \mp 1 \pmod{p};$$

folglich ist wenigstens eine der Zahlen a und $-a$ eine nicht primitive Wurzel.

Primitive Wurzeln einer Potenz einer ungeraden Primzahl, oder des Doppelten einer solchen Potenz.

317. Lehrsatz I. — Wenn p eine ungerade Primzahl und g eine primitive Wurzel von p^ν ist, so ist die Zahl g oder ihr nach p genommener Rest auch eine primitive Wurzel von p.

Bezeichnet nämlich n den Exponenten, zu welchem g in Beziehung auf p gehört, so hat man

$$g^n \equiv 1 \pmod{p},$$

oder

$$g^n = 1 + kp,$$

wo k eine ganze Zahl bedeutet. Wird diese Gleichung auf die p^{te} Potenz erhoben, so ergiebt sich

$$g^{np} = 1 + \frac{p}{1} kp + \frac{p(p-1)}{1.2} k^2 p^2 + \cdots.$$

Alle Terme des zweiten Gliedes dieser Formel, mit Ausnahme des ersten Terms, sind durch p^2 theilbar; wir können daher

$$g^{np} = 1 + k_1 p^2$$

setzen, wo unter k_1 eine ganze Zahl verstanden wird. Ebenso erhält man durch mehrmalige Erhebung auf die p^{te} Potenz

$$g^{np^2} = 1 + k_2 p^3,$$
$$\ldots\ldots\ldots\ldots,$$
$$g^{np^{\nu-1}} = 1 + k_{\nu-1} p^\nu;$$

$k_2, \ldots, k_{\nu-1}$ bezeichnen ganze Zahlen. Die letzte dieser Gleichungen lässt sich auf die Form

$$g^{np^{\nu-1}} \equiv 1 \pmod{p^\nu}$$

bringen und zeigt somit, dass g nur dann primitive Wurzel von p^ν sein kann, wenn $n = p - 1$ ist; in diesem Falle ist aber g primitive Wurzel von p.

318. Lehrsatz II. — Eine primitive Wurzel g der ungeraden Primzahl p ist auch primitive Wurzel von p^ν $(\nu > 1)$, wenn $\frac{g^{p-1}-1}{p}$ nicht durch p theilbar ist. Umgekehrt ist g keine primitive Wurzel von p^ν, wenn p in $\frac{g^{p-1}-1}{p}$ aufgeht.

Bezeichnet t den Exponenten, zu welchem g in Beziehung auf den Modul p^ν gehört, so ist

$$g^t \equiv 1 \pmod{p^\nu},$$

folglich auch

$$g^t \equiv 1 \pmod{p}.$$

Da g der Voraussetzung nach primitive Wurzel von p ist, so muss t der letzten Congruenz wegen ein Vielfaches von $p-1$ sein. Ausserdem ist t ein Divisor von

$$\varphi(p^\nu) = p^{\nu-1}(p-1),$$

mithin hat man

$$t = p^\lambda (p-1),$$

wo $\lambda <$ oder $= \nu - 1$ ist.

Dies vorausgesetzt, sei i der Exponent der höchsten Potenz von p, welche in $g^{p-1} - 1$ aufgeht; dann ist

$$g^{p-1} = 1 + k p^i,$$

wo k eine durch p nicht theilbare ganze Zahl bedeutet. Man erhält hieraus, wenn man beachtet, dass i von Null verschieden sein muss,

$$g^{p(p-1)} = 1 + k_1 p^{i+1},$$
$$g^{p^2(p-1)} = 1 + k_2 p^{i+2},$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot,$$
$$g^{p^\lambda(p-1)} = 1 + k_\lambda p^{i+\lambda};$$

darin sind $k_1, k_2, \ldots, k_\lambda$ durch p nicht theilbare ganze Zahlen. Aus diesen Formeln ist ersichtlich, dass

$$\lambda = \nu - i$$

der kleinste der Werthe von λ ist, für welche man

$$g^{p^\lambda(p-1)} \equiv 1 \pmod{p^\nu}$$

hat. Es ist daher

$$\lambda = \nu - 1 \text{ für } i = 1$$

und

$$\lambda < \nu - 1 \text{ für } i > 1.$$

Im ersteren Falle gehört g zum Exponenten $\varphi(p^\nu)$ in Beziehung auf den Modul p^ν, d. h. g ist eine primitive Wurzel. Im zweiten Falle gehört g zu einem Exponenten, der kleiner als $\varphi(p^\nu)$ ist, d. h. g ist keine primitive Wurzel.

319. Lehrsatz III. — Jeder primitiven Wurzel der Primzahl p entsprechen $p^{\nu-2}(p-1)$ primitive Wurzeln von p^ν.

Es sei a eine zwischen 0 und $p-1$ liegende primitive Wur-

zel von p; die der Wurzel a congruenten primitiven Wurzeln werden durch den Ausdruck

$$g = a + kp$$

gegeben, in welchem k irgend eine ganze Zahl ist; daraus folgt

$$g^{p-1} - 1 = (a^{p-1} - 1) + \frac{p-1}{1} a^{p-2} kp + \frac{(p-1)(p-2)}{1 \cdot 2} a^{p-3} k^2 p^2 + \cdots$$

Wir nehmen nun erstens an, $a^{p-1} - 1$ sei nicht durch p^2 theilbar. $g^{p-1} - 1$ ist durch p^2 theilbar oder nicht theilbar, jenachdem

$$\frac{a^{p-1} - 1}{p} + (p-1) a^{p-2} k \text{ oder } \frac{a^p - a}{p} - k$$

durch p theilbar ist oder nicht. Bezeichnet daher α den kleinsten Rest von $\frac{a^p - a}{p}$ in Beziehung auf p, und macht man

$$k = \alpha + h,$$

wo h eine durch p nicht theilbare Zahl ist, so sind nach dem Lehrsatz II alle in der Formel

$$(1). \qquad g = a + (\alpha + h) p$$

enthaltenen Zahlen g primitive Wurzeln von p^ν.

Ist zweitens $a^{p-1} - 1$ durch p^2 theilbar, so geht p^2 in $g^{p-1} - 1$ nur dann auf, wenn k durch p theilbar ist; daraus folgt, dass die Formel

$$(2). \qquad g = a + hp,$$

in welcher h eine durch p nicht theilbare Zahl ist, nur primitive Wurzeln von p^ν liefert. Will man nur die Werthe von g erhalten, welche nach dem Modul p^ν incongruent sind, so darf man der Grösse h in den Formeln (1) und (2) nur $\varphi(p^{\nu-1}) = p^{\nu-2}(p-1)$ verschiedene Werthe ertheilen; ebensoviele primitive Wurzeln ergeben sich dann für den Modul p^ν.

Anmerkung. — Da a primitive Wurzel von p ist, so kann die Zahl $a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$ nicht durch p theilbar sein, wofern nicht

$$a^{\frac{p-1}{2}} + 1 \equiv 0 \ (mod.\ p^2)$$

ist.

Zusatz. — Die Anzahl der primitiven Wurzeln von p^ν ist gleich $\varphi[p^{\nu-1}(p-1)]$ oder gleich $\varphi\varphi(p^\nu)$.

Nach dem Lehrsatz I ist nämlich jede primitive Wurzel von p^ν auch primitive Wurzel von p; ferner liefert jede der $\varphi(p-1)$ primitiven Wurzeln von p, wie der vorhergehende Lehrsatz aussagt,

$\varphi(p^{\nu-1})$ primitive Wurzeln von p^ν. Die Gesammtzahl der letzteren ist somit

$$\varphi(p^{\nu-1}) \cdot \varphi(p-1) = \varphi[p^{\nu-1}(p-1)] = \varphi\varphi(p^\nu).$$

320. Lehrsatz IV. — Wenn p eine ungerade Primzahl bezeichnet, so ist jede ungerade primitive Wurzel von p^ν zugleich primitive Wurzel von $2p^\nu$, und umgekehrt ist jede primitive Wurzel von $2p^\nu$ auch primitive Wurzel von p^ν.

Es sei g eine ungerade, durch p nicht theilbare Zahl, und es mögen n, n' die Exponenten sein, zu welchen g beziehungsweise nach den Moduln p^ν, $2p^\nu$ gehört; dann hat man

(1). $$g^n \equiv 1 \ (mod.\ p^\nu)\ ,\ g^{n'} \equiv 1 \ (mod.\ 2p^\nu).$$

Die zweite dieser Congruenzen liefert

(2). $$g^{n'} \equiv 1 \ (mod.\ p^\nu),$$

folglich ist n' ein Vielfaches von n. Da ausserdem g eine ungerade Zahl ist, so ist $g^n \equiv 1 \ (mod.\ 2)$; die erste der Congruenzen (1) liefert daher auch

$$g^n \equiv 1 \ (mod.\ 2p^\nu),$$

und dieser Congruenz wegen muss n ein Vielfaches von n' sein. Man hat somit $n = n'$, und die Zahl g gehört in Beziehung auf die Moduln p^ν, $2p^\nu$ zu ein und demselben Exponenten.

Da nun

$$\varphi(2p^\nu) = \varphi(p^\nu) = p^{\nu-1}(p-1),$$

so ist die Zahl g eine primitive Wurzel für den einen der Moduln $2p^\nu$, p^ν, wenn sie es für den andern ist.

Zusatz. — Es giebt ebenso viele primitive Wurzeln für den Modul $2p^\nu$, als für den Modul p^ν.

Nimmt man nämlich die ungeraden primitiven Wurzeln von p^ν und fügt die geraden hinzu, nachdem man jede der letzteren um p^ν vermehrt hat, so erhält man $\varphi\varphi(p^\nu)$ primitive Wurzeln von $2p^\nu$.

321. Beispiel. — Betrachten wir den Fall $p = 7$. Die primitiven Wurzeln von 7 sind 3 und 5; man hat

$$3^3 = 27\ ,\ 5^3 = 125 \equiv 27 \ (mod.\ 49);$$

folglich sind 3 und 5 primitive Wurzeln von 7^ν und $2 \times 7^\nu$ für jeden Werth des Exponenten ν.

Wir setzen $\nu = 2$ voraus, und suchen zunächst die primitiven Wurzeln von 49. Da

$$\frac{3^7 - 3}{7} = 312 \equiv 4, \frac{5^7 - 5}{7} = 11160 \equiv 2 \ (mod.\ 7)$$

ist, so hat die in No. 319 mit α bezeichnete Zahl beziehungsweise die Werthe 4 und 2. Die primitiven Wurzeln von 49 werden daher durch die Formeln

$$g = 3 + 7\ (h + 4)\ ,\ g = 5 + 7\ (h + 2)$$

gegeben, worin h prim zu 7 sein muss. Ertheilt man dieser unbestimmten Grösse in der ersten Formel die Werthe

$$-4\ ,\ -3\ ,\ -2\ ,\ -1\ ,\ +1\ ,\ +2\ ,$$

in der zweiten Formel die Werthe

$$-2\ ,\ -1\ ,\ +1\ ,\ +2\ ,\ +3\ ,\ +4\ ,$$

so erhält man die beiden folgenden Reihen, deren jede aus sechs Wurzeln besteht:

$$\begin{array}{cccccc} 3 & ,\ 10 & ,\ 17 & ,\ 24 & ,\ 38 & ,\ 45, \\ 5 & ,\ 12 & ,\ 26 & ,\ 33 & ,\ 40 & ,\ 47, \end{array}$$

oder

$$\begin{array}{cccccc} 3 & ,\ 3^{13} & ,\ 3^{25} & ,\ 3^{37} & ,\ 3^{19} & ,\ 3^{31}, \\ 3^{29} & ,\ 3^{11} & ,\ 3^{17} & ,\ 3^{41} & ,\ 3^{23} & ,\ 3^{5}. \end{array}$$

Was ferner den Modul 2×49 oder 98 betrifft, so besitzt derselbe die zwölf primitiven Wurzeln

$$\begin{array}{cccccc} 3\ , & 17\ , & 45\ , & 59\ , & 73\ , & 87, \\ 5\ , & 33\ , & 47\ , & 61\ , & 75\ , & 89. \end{array}$$

Ueber die Congruenz $x^t - 1 \equiv 0\ (mod.\ M)$, im Falle M eine Potenz einer ungeraden Primzahl oder das Doppelte einer solchen Potenz ist.

322. Es sei p eine ungerade Primzahl, und a eine Wurzel der Congruenz

(1). $$x^t - 1 \equiv 0\ (mod.\ p^\nu \text{ oder } 2\,p^\nu);$$

dann ist gleichzeitig

$$a^t \equiv 1\ ,\ a^{p^{\nu-1}(p-1)} \equiv 1\ (mod.\ p^\nu \text{ oder } 2\,p^\nu).$$

Bezeichnet daher ϑ den Exponenten, zu welchem a in Beziehung auf den Modul $M = p^\nu$ oder $= 2\,p^\nu$ gehört, so ist ϑ ein gemeinschaftlicher Divisor der Zahlen

$$t\ ,\ p^{\nu-1}\,(p-1)\,,$$

und muss folglich in den grössten gemeinschaftlichen Divisor n dieser Zahlen aufgehen. Da nun

$$a^{\vartheta} \equiv 1 \ (mod.\ p^{\nu} \text{ oder } 2\,p^{\nu})$$

ist, so muss auch

$$a^{n} \equiv 1 \ (mod.\ p^{\nu} \text{ oder } 2\,p^{\nu})$$

sein, und daraus geht hervor, dass alle Wurzeln der vorgelegten Congruenz auch der Congruenz

$$(2).\qquad x^{n} - 1 \equiv 0 \ (mod.\ p^{\nu} \text{ oder } 2\,p^{\nu})$$

angehören, deren Grad n ein Divisor von $p^{\nu-1}(p-1)$ ist. Wenn $n = p^{\nu-1}(p-1)$ ist, so geht die Congruenz (2) über in

$$(3).\qquad x^{p^{\nu-1}(p-1)} - 1 \equiv 0 \ (mod.\ p^{\nu} \text{ oder } 2\,p^{\nu})$$

und hat, wie wir wissen, die $p^{\nu-1}(p-1)$ Zahlen zu Wurzeln, welche prim zum Modul und nicht grösser als der Modul sind. Unter diesen Wurzeln befinden sich $\varphi\,[p^{\nu-1}(p-1)]$ primitive, deren Ermittlung wir oben gelehrt haben. Bezeichnet a eine dieser primitiven Wurzeln, so sind die kleinsten Reste der Potenzen

$$(4).\qquad 1\ ,\ a\ ,\ a^2\ ,\ a^3\ ,\ \ldots\ ,\ a^{p^{\nu-1}(p-1)}$$

die Wurzeln der Congruenz (3).

Wir nehmen jetzt an, n sei irgend ein Divisor von $p^{\nu-1}(p-1)$, setzen

$$p^{\nu}\,(p-1) = n\vartheta$$

und betrachten irgend einen Term a^m der Reihe (4). Damit

$$(a^m)^n \equiv 1 \text{ oder } a^{mn} \equiv 1 \ (mod.\ p^{\nu} \text{ oder } 2\,p^{\nu})$$

sei, ist erforderlich und hinreichend, dass $n\vartheta$ in mn aufgehe, d. h. dass m ein Vielfaches von ϑ sei. Daher hat die Congruenz (2) genau n Wurzeln, und es sind dies die nach dem Modul p^{ν} oder $2\,p^{\nu}$ genommenen Reste der Potenzen

$$(5).\qquad a^{\vartheta}\ ,\ a^{2\vartheta}\ ,\ \ldots\ ,\ a^{n\vartheta}.$$

Man erhält auf diese Weise den

Lehrsatz I. — Die Congruenz $x^t - 1 \equiv 0$ ($mod.\ p^{\nu}$ oder $2\,p^{\nu}$) hat so viele Wurzeln, als der grösste gemeinschaftliche Divisor der beiden Zahlen t und $p^{\nu-1}(p-1)$ Einheiten enthält.

Es sei ferner $a^{i\vartheta}$ irgend ein Term der Reihe (5). Damit man

$$(a^{i\vartheta})^k = a^{ki\vartheta} \equiv 1 \ (mod.\ p^\nu \text{ oder } 2\,p^\nu)$$

habe, ist erforderlich und hinreichend, dass $ki\vartheta$ durch $n\vartheta$, oder ki durch n theilbar sei. Wenn i prim zu n ist, so wird diese Bedingung nur dann erfüllt, wenn n in k aufgeht; in diesem Falle gehört $a^{i\vartheta}$ offenbar zum Exponenten n. Haben aber i und n einen grössten gemeinschaftlichen Divisor d, der > 1 ist, so hat man

$$(a^{i\vartheta})^{\frac{n}{d}} = (a^{\frac{i}{d}})^{n\vartheta} \equiv 1 \ (mod.\ p^\nu \text{ oder } 2\,p^\nu),$$

und $a^{i\vartheta}$ gehört zum Exponenten $\frac{n}{d}$. Daraus ergiebt sich der folgende Satz:

Lehrsatz II. — Die Congruenz $x^n \equiv 1$ ($mod.\ p^\nu$ oder $2\,p^\nu$), deren Grad n ein Divisor von $p^{\nu-1}(p-1)$ ist, hat so viele primitive, d. h. zum Exponenten n gehörende Wurzeln, als es Zahlen giebt, die prim zu n und nicht grösser als n sind.

Der Modul 2^ν.

323. In No. 305 haben wir gesehen, dass, sobald man $\nu > 2$ voraussetzt, schon die $(2^{\nu-2})^{\text{te}}$ Potenz jeder ungeraden Zahl nach dem Modul 2^ν der Einheit congruent ist. Nur für $\nu = 2$ findet eine Ausnahme statt, da es in diesem Falle wirklich eine primitive Wurzel, nämlich 3, giebt.

Wir nehmen jetzt an, ν sei grösser als 2; dann ist der Exponent, zu welchem irgend eine ungerade Zahl in Beziehung auf den Modul 2^ν gehört, eine Potenz von 2, deren Grad $=$ oder $< \nu - 2$ ist.

Die Zahl 1 ist die einzige, welche zum Exponenten 1 gehört; wir beschäftigen uns nur mit denjenigen ungeraden Zahlen, welche grösser als 1 sind. Jede derselben kann durch die Formel

(1). $$a = 2^{i+2}\,k \pm 1$$

dargestellt werden, in welcher k eine ungerade Zahl und i einen Exponenten bezeichnet, der auch Null sein kann. Aus (1) ergiebt sich leicht die Reihe der Formeln

$$(2). \quad \begin{cases} a^2 = 2^{i+3} k_1 + 1, \\ a^{2^2} = 2^{i+4} k_2 + 1, \\ \dots\dots\dots\dots\dots, \\ a^{2^\delta} = 2^{i+2+\delta} k_\delta + 1, \end{cases}$$

in welchen k_1, k_2, ..., k_δ ungerade Zahlen bedeuten.

Ist 2^δ der Exponent, zu welchem die Zahl a gehört, so hat man

$$i + 2 + \delta = \text{oder} > \nu;$$

wenn $\delta > 1$ ist, so kann $i + 2 + \delta$ nicht $> \nu$ sein, da sonst den Formeln (2) zufolge $a^{2^{\delta-1}} - 1$ durch 2^ν theilbar, also der Exponent, zu welchem a gehört, kleiner als 2^δ wäre. Es ist daher

$$i + 2 = \nu - \delta,$$

und die Formel (1) geht über in

$$(3). \quad a = 2^{\nu-\delta} k \pm 1.$$

Man kann k die $2^{\delta-1}$ Werthe

$$1, 3, 5, \dots, (2^\delta - 1)$$

ertheilen und erhält des doppelten Zeichens $\pm$ wegen für a zwei Reihen von Werthen, deren jede aus $2^{\delta-1}$ Termen besteht; es ergiebt sich somit der

Lehrsatz. — Bezeichnet δ eine der Zahlen 2, 3, 4, ..., $(\nu-2)$, so giebt es 2^δ Zahlen, welche in Beziehung auf den Modul 2^ν zum Exponenten 2^δ gehören.

Wenn die schon betrachtete Zahl a zum Exponenten 2 gehört, so liefert die erste der Formeln (2)

$$i + 3 = \text{oder} > \nu, \quad i + 2 = \text{oder} > \nu - 1.$$

Nimmt man aber $i + 2 = \nu$, so muss, da a der Voraussetzung nach kleiner als der Modul 2^ν ist, in der Formel (1) $k = 1$ gemacht und das Zeichen $\pm$ durch $-$ ersetzt werden; es giebt daher drei zum Exponenten 2 gehörende Zahlen, nämlich

$$(4). \quad 2^{\nu-1} - 1, \quad 2^{\nu-1} + 1, \quad 2^\nu - 1.$$

Die Zahlen, welche zum höchsten im vorliegenden Falle in Betracht kommenden Exponenten, nämlich zu $2^{\nu-2}$ gehören, werden dadurch erhalten, dass man in der Formel (3) $\delta = \nu - 2$ macht. Ersetzt man zugleich k durch $2k + 1$, so erhält man die beiden Formeln

$$a = 8k + 3 \text{ , } a = 8k + 5,$$

welche alle zum Exponenten $2^{\nu-2}$ gehörenden Zahlen liefern. Es wird hierbei aber vorausgesetzt, dass $\nu > 3$ sei; denn für $\nu = 3$ sind die zum Exponenten $2^{\nu-2} = 2$ gehörenden Zahlen den Formeln (4) zufolge

$$3 \text{ , } 5 \text{ , } 7.$$

Wir lassen diesen Fall bei Seite und bezeichnen, $\nu > 3$ vorausgesetzt, mit b irgend eine Zahl von der Form $8k + 3$, mit c irgend eine Zahl von der Form $8k + 5$. Jede der beiden Reihen

$$b \text{ , } b^2 \text{ , } \ldots \text{ , } b^{2^{\nu-2}},$$
$$c \text{ , } c^2 \text{ , } \ldots \text{ , } c^{2^{\nu-2}}$$

liefert $2^{\nu-2}$ verschiedene Reste, da b und c zum Exponenten $2^{\nu-2}$ gehören. Ausserdem sind die ungeraden Potenzen von b und von c beziehungsweise von den Formen $8k + 3$, $8k + 5$, während die geraden Potenzen sowohl von b, als auch von c die Form $8k + 1$ haben. Da es nun zwischen den Grenzen 1 und $2^\nu - 1$ $2^{\nu-3}$ Zahlen von jeder der Formen

$$8k + 1 \text{ , } 8k + 3 \text{ , } 8k + 5 \text{ , } 8k + 7$$

giebt, so liefert die Reihe der Potenzen von b alle Zahlen $8k + 3$ und $8k + 1$, während in der Reihe der Potenzen von c sich alle Zahlen $8k + 5$ und nochmals alle Zahlen $8k + 1$ vorfinden.

Aendert man die Zeichen der Zahlen $8k + 1$ und $8k + 5$ oder nimmt deren Ergänzungen zum Modul 2^ν, so erhält man offenbar alle Zahlen $8k + 7$ und $8k + 3$; man gelangt also zu dem folgenden Satze:

Lehrsatz. — Wählt man irgend eine Zahl von der Form $8k + 3$ oder $8k + 5$, nimmt in Beziehung auf den Modul 2^ν die Reste der $2^{\nu-2}$ ersten Potenzen derselben und fügt hinzu die Ergänzungen dieser Reste zum Modul, so erhält man die Reihe aller ungeraden Zahlen, welche kleiner als der Modul sind.

Ueber die Congruenz $x^t - 1 \equiv 0 \pmod{2^\nu}$.

324. Wir betrachten die Congruenz

$$(1). \qquad x^t - 1 \equiv 0 \pmod{2^\nu},$$

in welcher $\nu > 2$ ist. Für jede Wurzel a derselben hat man

$$a^t \equiv 1 \; , \; a^{2^{\nu-2}} \equiv 1 \quad (mod.\ 2^\nu);$$

daher muss der Exponent, zu welchem a gehört, in t und in $2^{\nu-2}$, sowie in den grössten gemeinschaftlichen Divisor dieser Zahlen aufgehen. Wir bezeichnen diesen grössten gemeinschaftlichen Divisor mit 2^δ; dann ist a eine Wurzel der Congruenz

(2). $$x^{2^\delta} - 1 \equiv 0 \quad (mod.\ 2^\nu),$$

und umgekehrt genügen alle Wurzeln von (2) auch der vorgelegten Congruenz (1). Die Wurzeln von (2) sind offenbar nichts Anderes, als die Zahlen, welche zu einem der Exponenten

$$1 \; , \; 2 \; , \; 2^2 \; , \; \ldots \; , \; 2^\delta$$

gehören.

Wenn t eine ungerade Zahl ist, so hat man $\delta = 0$, und die Congruenzen (1) und (2) besitzen keine andere Wurzel als 1. Setzen wir $\delta > 0$ voraus; wir haben oben gesehen, dass, wenn $\mu > 1$ ist, es 2^μ zum Exponenten 2^μ gehörende Zahlen giebt, und dass 3 Zahlen zum Exponenten 2 gehören; die Congruenz (2) hat daher

$$1 + 3 + 2^2 + 2^3 + \cdots + 2^\delta$$

oder $2^{\delta+1}$ Wurzeln, und wir erhalten den Satz:

Lehrsatz. — Wenn t eine gerade Zahl ist, so hat die Congruenz $x^t - 1 \equiv 0$ $(mod.\ 2^\nu)$ doppelt so viele Wurzeln, als der grösste gemeinschaftliche Divisor der Zahlen t und $2^{\nu-2}$ Einheiten enthält.

Diese Wurzeln bilden zwei Perioden. Bezeichnen wir nämlich mit c eine zum Exponenten $2^{\nu-2}$ gehörende Zahl und setzen

$$a \equiv c^{2^{\nu-2-\delta}} \quad (mod.\ 2^\nu),$$

so können die Wurzeln der Congruenzen (1) und (2) nach den vorhergehenden Entwicklungen offenbar durch

$$a \; , \quad a^2 \; , \quad a^3 \; , \; \ldots \; , \quad a^{2^\delta} \; ,$$
$$-a \; , \; -a^2 \; , \; -a^3 \; , \; \ldots \; , \; -a^{2^\delta}$$

dargestellt werden.

Ueber die Congruenz $x^t \equiv 1$, wenn der Modul eine beliebige Zahl ist.

325. Die Congruenz

(1). $$x^t - 1 \equiv 0 \; (mod.\ M),$$

deren Modul M eine beliebig zusammengesetzte Zahl ist, lässt sich leicht auf die bisher betrachteten Fälle zurückführen.

Es sei

$$M = p^\nu\, q^\mu\, r^\lambda \ldots,$$

wo $p, q, r, \ldots$ ungleiche Primzahlen bezeichnen. Offenbar muss jede Wurzel der vorgelegten Congruenz derselben Congruenz

$$(2). \qquad x^t - 1 \equiv 0$$

nach jedem der Moduln $p^\nu, q^\mu, r^\lambda, \ldots$ genügen. Wenn umgekehrt $a, b, c, \ldots$ beziehungsweise Wurzeln der Congruenz (2) nach den Moduln $p^\nu, q^\mu, r^\lambda, \ldots$ sind, und wenn die Zahl x so bestimmt wird, dass man

$$x \equiv a \ (mod.\ p^\nu),$$
$$x \equiv b \ (mod.\ q^\mu),$$
$$x \equiv c \ (mod.\ r^\lambda),$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

hat, so befriedigt x die Congruenz (2) in Beziehung auf jeden der Moduln $p^\nu, q^\mu, r^\lambda, \ldots$, folglich auch in Beziehung auf den Modul M.

Die Ermittlung der Wurzeln der vorgelegten Congruenz (1) ist somit auf die Auflösung von Congruenzen zurückgeführt, deren Modul eine Potenz einer Primzahl ist; diese Aufgabe haben wir aber bereits in No. 290 erledigt.

Indices.

326. Das Vorhandensein von primitiven Wurzeln für einen Modul M, der gleich einer Potenz einer Primzahl oder gleich dem Doppelten einer solchen Potenz ist, zieht äusserst wichtige Folgen nach sich, mit denen wir uns jetzt zu beschäftigen haben.

Ist a irgend eine der primitiven Wurzeln, so liefern die Potenzen von a alle Zahlen, die prim zum Modul sind. Bezeichnet daher N eine dieser Zahlen, so hat man für gewisse Werthe von n

$$a^n \equiv N \ (mod.\ M).$$

Jede der so bestimmten Zahlen n heisst der Index von N; die primitive Wurzel a wird die Basis der Indices genannt.

Eine Zahl hat eine unendliche Menge Indices, die jedoch

sämmtlich nach dem Modul $\varphi(M)$ congruent sind. Man kann sich daher auf die Betrachtung des kleinsten Index, welcher ein Term der Reihe

$$0, 1, 2, \ldots, \varphi(M) - 1$$

ist, beschränken. Der kleinste Index der Einheit ist offenbar Null.

Hat man die Indices der Zahlen N, die prim zu M sind, für die Basis a berechnet, so lassen sich daraus die auf eine andere primitive Wurzel a' als Basis bezüglichen Indices leicht herleiten. Ist nämlich e der Index der neuen Basis a' im ersten System, so hat man

$$a' \equiv a^e \ (mod.\ M),$$

und wenn eine Zahl N für die Basis a den Index n, für die Basis a' den Index n' hat, so ist

$$a'^{n'} \equiv a^n \ (mod.\ M),$$

oder

$$a^{n'e} \equiv a^n \ (mod.\ M);$$

dies erfordert aber, dass

$$n'e \equiv n \ [mod.\ \varphi(M)],$$

oder, da e prim zu $\varphi(M)$ ist, dass

$$n' \equiv \frac{n}{e} \left[mod.\ \varphi(M)\right]$$

sei. Die neuen Indices werden also dadurch erhalten, dass man die alten durch den auf das erste System bezüglichen Index der neuen Basis dividirt.

327. Die Eigenschaften der Indices sind denjenigen der Logarithmen ganz analog; sie ergeben sich sämmtlich aus dem folgenden Satze:

Lehrsatz. — Der nach dem Modul M genommene Index eines Produkts mehrerer Factoren ist nach dem Modul $\varphi(M)$ der Summe der Indices der Factoren congruent.

Es seien in dem Systeme, dessen Basis a ist, $\alpha, \beta, \gamma, \ldots$ die Indices der Zahlen $A, B, C, \ldots$; dann ist

$$a^\alpha \equiv A, \ a^\beta \equiv B, \ a^\gamma \equiv C, \ \ldots \ (mod.\ M.),$$

und durch Multiplication dieser Congruenzen erhält man

$$a^{\alpha+\beta+\gamma+\cdots} \equiv ABC \ldots \ (mod.\ M),$$

woraus hervorgeht, dass der kleinste Index des Produkts $ABC\ldots$ der nach $\varphi(M)$ genommene Rest von $\alpha + \beta + \gamma + \cdots$ ist. Man hat daher

$$ind.\,(ABC\ldots) \equiv ind.\,A + ind.\,B + ind.\,C + \ldots\ [mod.\ \varphi(M)].$$

Zusatz I. — Der nach dem Modul M genommene Index einer Potenz einer Zahl ist nach dem Modul $\varphi(M)$ dem Produkte aus dem Index der Zahl in den Exponenten der Potenz congruent.

Zusatz II. — Der nach dem Modul M genommene Index des Quotienten zweier Zahlen ist nach dem Modul $\varphi(M)$ der Differenz zwischen dem Index des Zählers und demjenigen des Nenners congruent.

Da nämlich

$$\frac{A}{B} \times B = A$$

ist, so hat man

$$ind.\,\frac{A}{B} + ind.\,B \equiv ind.\,A\ \left[mod.\ \varphi(M)\right],$$

oder

$$ind.\,\frac{A}{B} \equiv ind.\,A - ind.\,B\ \left[mod.\ \varphi(M)\right].$$

Man ersieht hieraus, dass, wenn man zwei Tabellen hat, von denen die eine die Indices der Zahlen für jeden Modul, die andere die Zahlen kennen lehrt, welche gegebenen Indices entsprechen, man die Congruenzen ersten Grades mit Leichtigkeit auflösen kann, da dieselben sich auf andere Congruenzen zurückführen lassen, deren Moduln Primzahlen oder Potenzen von Primzahlen sind.

Benutzung der Indices zur Auflösung der binomischen Congruenzen.

328. Die Wurzeln der binomischen Congruenz

(1). $$x^t \equiv A\ (mod.\ M)$$

können, wenn man will, durch die Formel

(2). $$x \equiv \sqrt[t]{A}\ (mod.\ M)$$

dargestellt werden; der Modul M ist, wie früher, eine Potenz einer ungeraden Primzahl oder das Doppelte einer solchen Potenz. Es

handelt sich darum, die in dem Symbol $\sqrt[t]{A}$ (*mod. M*) enthaltenen Zahlen zu bestimmen.

Nach dem Vorhergehenden ist die Congruenz (1) mit

$$(3). \qquad t \cdot ind.\, x \equiv ind.\, A\ [mod.\ \varphi(M)]$$

gleichbedeutend; wenn man daher eine Indextafel (Jacobi, Canon Arithmeticus, 1839) besitzt, so hat man nur noch eine Congruenz ersten Grades zu lösen.

Wenn t prim zu $\varphi(M)$ ist, so liefert die Congruenz (3) für *ind.* x nur einen Werth, und die vorgelegte Congruenz besitzt folglich nur eine Wurzel. Wenn aber t und $\varphi(M)$ einen grössten gemeinschaftlichen Divisor $\delta > 1$ haben, so ist die Congruenz (3) nur dann möglich, wenn δ auch in *ind.* A aufgeht, und in diesem Falle besitzt die vorgelegte Congruenz (1) δ Wurzeln.

Ist z. B. $A = 1$, also die vorgelegte Congruenz

$$x^t \equiv 1\ (mod.\ p^\nu \text{ oder } 2p^\nu),$$

so ergiebt sich

$$t \cdot ind.\, x \equiv 0\ [mod.\ p^{\nu-1}(p-1)].$$

Bezeichnet daher δ den grössten gemeinschaftlichen Divisor von t und $p^{\nu-1}(p-1)$, so erhält man folgende δ Werthe für *ind.* x:

$$ind.\, x = \frac{(p-1)\,p^{\nu-1}}{\delta},\ 2\,\frac{(p-1)\,p^{\nu-1}}{\delta},\ \ldots,\ \delta\,\frac{(p-1)\,p^{\nu-1}}{\delta},$$

und jedem derselben entspricht ein aus der Indextafel zu entnehmender Werth von x.

Beweis eines Satzes von Lagrange.

329. Es würde uns zu weit führen, alle Folgerungen hier darzulegen, die man aus der im Vorhergehenden entwickelten Theorie ziehen kann. Wir wollen indess zwei Anwendungen derselben machen, von denen die erste den Beweis eines wichtigen Satzes von Lagrange zum Gegenstand hat. Dieser Beweis stützt sich auf den folgenden

Hilfssatz. — Wenn die Primzahl p grösser als 5 ist, so giebt es in der Reihe

$$1, 2, 3, \ldots, (p-1)$$

1⁰ einen quadratischen Rest, auf welchen ein Nichtrest folgt; 2⁰ einen Nichtrest, auf welchen ein Rest

folgt; 3^0 zwei aufeinander folgende Reste; 4^0 zwei aufeinander folgende Nichtreste.

1^0. Da der erste Term 1 ein Rest ist, und da ebenso viele Reste als Nichtreste vorhanden sind, so muss es einen Rest geben, auf welchen ein Nichtrest folgt.

2^0. Gäbe es keinen Nichtrest, dem ein Rest folgte, so würden die $\frac{p-1}{2}$ ersten Terme Reste, die $\frac{p-1}{2}$ letzten Terme Nichtreste sein. Wäre aber jede der beiden Zahlen 2 und $\frac{p-1}{2}$ ein Rest, so müsste auch ihr Produkt $p-1$ ein Rest sein, und dass steht, sobald $p > 5$ ist, mit dem Vorhergehenden im Widerspruch.

3^0. Es giebt zwei aufeinander folgende Reste. Da für $p = 7$ jede der Zahlen 1 und 2 ein Rest ist, so können wir $p =$ oder > 11 voraussetzen. Ist nun eine der Zahlen 2, 3, 5 ein Rest, so ist der Satz bewiesen, da 1 und 4 stets Reste sind; sind diese drei Zahlen aber sämmtlich Nichtreste, so ist das Produkt 2×5 oder 10, ebenso wie 9, ein Rest.

4^0. Es giebt zwei aufeinanderfolgende Nichtreste. Wir haben uns eben von der Existenz zweier aufeinander folgenden Reste überzeugt. Es sei a der kleinste Rest, auf welchen ein Rest $a+1$ folgt; sind dann zwischen 1 und a nicht zwei aufeinander folgende Nichtreste enthalten, so sind die Zahlen von 1 bis $a-1$ abwechselnd Reste und Nichtreste. Da ausserdem a und $a+1$ Reste sind, so muss von $a+1$ an die Anzahl der Nichtreste um zwei Einheiten grösser sein, als die Anzahl der Reste; dies erfordert aber, dass wenigstens zwei aufeinander folgende Terme Nichtreste seien.

Anmerkung. — Der Satz darf nicht auf den Fall $p = 5$ bezogen werden, da in der Reihe 1, 2, 3, 4 die Zahlen 1, 4 Reste, die Zahlen 2, 3 Nichtreste sind.

Zusatz. — Bezeichnet C irgend eine durch p nicht theilbare Zahl, so gilt der vorstehende Satz auch dann noch, wenn statt der Reihe

(1). $$1, 2, 3, \ldots, (p-1)$$

die folgende:

(2). $$C, 2C, 3C, \ldots, (p-1)C$$

genommen wird.

Ist nämlich C ein Rest, so sind zwei entsprechende Terme der Reihen (1) und (2) gleichzeitig Reste oder Nichtreste. Ist aber C ein Nichtrest, so entsprechen die Reste von (1) den Nichtresten von (2), und umgekehrt.

330. Lehrsatz. — Wenn die Primzahl p grösser als 5 ist, und A, B, C drei durch p nicht theilbare positive oder negative ganze Zahlen bezeichnen, so lassen sich immer zwei ganze Zahlen t und u ermitteln, die kleiner als $\frac{p}{2}$ und von der Beschaffenheit sind, dass

$$At^2 + Bu^2 + C$$

durch p theilbar ist.

1⁰. Wenn die Zahlen B und $-C$ beide quadratische Reste, oder beide Nichtreste von p sind, so kann man $t = 0$ nehmen; dann hat man nämlich nur noch der Congruenz

$$Bu^2 + C \equiv 0 \ (mod.\ p), \text{ oder } Bu^2 + (C + \lambda p) \equiv 0 \ (mod.\ p)$$

zu genügen, worin λ irgend eine ganze Zahl ist. Wird λ so bestimmt, dass

$$-\frac{C + \lambda p}{B}$$

gleich einer ganzen Zahl μ wird, so geht unsere Congruenz über in

$$u^2 \equiv \mu \ (mod.\ p),$$

und diese Congruenz ist immer zu befriedigen; denn weil die Zahlen B und $-C$ beide Reste oder beide Nichtreste sind, so muss μ ein Rest von p sein.

Sind die Zahlen A und $-C$ beide Reste oder beide Nichtreste, so kann man der angegebenen Bedingung für jeden Werth der Primzahl p dadurch genügen, dass man $u = 0$ annimmt.

2⁰. Wenn $p > 5$ ist, so kann man der Congruenz

$$At^2 + Bu^2 + C \equiv 0 \ (mod.\ p)$$

immer durch positive Werthe von t und u genügen, die kleiner als $\frac{p}{2}$ sind. Es seien α und β zwei Zahlen, welche beziehungsweise von derselben Art wie $+A$ und $-B$ sind; wir sagen, zwei Zahlen seien von derselben Art, wenn beide Reste oder beide Nichtreste sind. Nach dem vorausgeschickten Hilfssatze kann man α und β so wählen, dass

$$\beta - \alpha \equiv C \ (mod.\ p)$$

ist, und wenn λ und μ solche ganze Zahlen bezeichnen, dass

$$\frac{\alpha + p\lambda}{A}, \quad \frac{\beta + p\mu}{-B}$$

ganze Zahlen sind, so sind diese ganzen Zahlen offenbar Reste von p; man hat daher

$$\frac{\alpha + p\lambda}{A} \equiv t^2, \quad \frac{\beta + p\mu}{-B} \equiv u^2 \ (mod.\ p),$$

oder

$$\alpha \equiv At^2, \quad \beta \equiv -Bu^2 \ (mod.\ p),$$

und da $\beta - \alpha \equiv C \ (mod.\ p)$ ist, so ergiebt sich

$$At^2 + Bu^2 + C \equiv 0 \ (mod.\ p), \text{ w. z. b. w.}$$

Anmerkung. — Nach diesem Satze umfasst die Formel

$$t^2 + u^2 + 1,$$

wenn $p > 5$ ist, Zahlen, welche durch p theilbar sind. Dasselbe findet aber auch noch im Falle $p = 5$ für $t = 0$, $u = 2$, im Falle $p = 3$ für $t = u = 1$ und im Falle $p = 2$ für $t = 0$, $u = 1$ statt. Da ausserdem die Formel $t^2 + u^2 + 1$ in der allgemeineren

$$P^2 + Q^2 + R^2 + S^2$$

enthalten ist, so sehen wir, dass jede Primzahl in eine Summe von vier Quadraten aufgeht, welche prim zu einander sind.

331. Dies Ergebniss wird uns zu einer wichtigen Folgerung führen, die einen Zusatz zum folgenden Satze bildet:

Lehrsatz. — Jede Zahl, welche in die Summe von vier Quadraten aufgeht, die prim zu einander sind, ist selbst die Summe von vier Quadraten.

Wir nehmen an, p gehe in

$$A^2 + B^2 + C^2 + D^2$$

auf, und bezeichnen mit $\pm a$, $\pm b$, $\pm c$, $\pm d$ die kleinsten Reste der Zahlen A, B, C, D, so dass a, b, c, d zwischen 0 und $\frac{p}{2}$ liegen. Dann ist p ein Divisor von

$$a^2 + b^2 + c^2 + d^2,$$

und wir können

$$(1). \qquad a^2 + b^2 + c^2 + d^2 = pp'$$

setzen. Da jede der Zahlen a, b, c, d kleiner als $\frac{p}{2}$ ist, so muss

$$pp' < 4\left(\frac{p}{2}\right)^2,$$

oder

$$p' < p$$

sein. Hätte man $p' = 1$, so würde p die Summe von vier Quadraten, unser Satz somit bewiesen sein; wir setzen also $p' > 1$ voraus. Da p' ein Divisor von $a^2 + b^2 + c^2 + d^2$ ist, so geht p' auch in die Summe der vier Quadrate

$$(a - \alpha p')^2 + (b - \beta p')^2 + (c - \gamma p')^2 + (d - \delta p')^2$$

auf; bestimmt man daher $\alpha, \beta, \gamma, \delta$ so, dass jedes dieser Quadrate kleiner als $\frac{p'^2}{4}$ ist, so hat man

$$(2).\quad (a - \alpha p')^2 + (b - \beta p')^2 + (c - \gamma p')^2 + (d - \delta p')^2 = p' p''$$

und zugleich

$$p'' < p'.$$

Durch Multiplication der Gleichungen (1) und (2) und durch Benutzung der in No. 245 hergeleiteten Formel ergiebt sich

$$(a\delta - b\gamma + c\beta - d\alpha)^2 p'^2 + (a\gamma + b\delta - c\alpha - d\beta)^2 p'^2$$
$$+ (a\beta - b\alpha - c\delta + d\gamma)^2 p'^2$$
$$+ [a^2 + b^2 + c^2 + d^2 - (a\alpha + b\beta + c\gamma + d\delta) p']^2 = pp'^2 p''.$$

Wird diese Gleichung durch p'^2 dividirt, so folgt mit Rücksicht auf (1):

$$(a\delta - b\gamma + c\beta - d\alpha)^2 + (a\gamma + b\delta - c\alpha - d\beta)^2$$
$$+ (a\beta - b\alpha - c\delta + d\gamma)^2 + (p - a\alpha - b\beta - c\gamma - d\delta)^2 = pp'',$$

oder kurz

$$(3).\quad a'^2 + b'^2 + c'^2 + d'^2 = pp''.$$

Diese Gleichung (3) hat dieselbe Form, wie (1); nur ist $p'' < p'$. Hat man $p'' = 1$, so lehrt (3), dass p die Summe von vier Quadraten ist, und unser Satz ist bewiesen. Ist aber $p'' > 1$, so verfahren wir mit der Gleichung (3) ebenso, wie wir mit (1) verfuhren. Dadurch gelangen wir zu einer neuen Gleichung von der Form

$$a''^2 + b''^2 + c''^2 + d''^2 = pp''',$$

wo

$$p''' < p''$$

ist. Diese Operationen setzen wir so lange fort, bis wir eine Gleichung von der Form

$$a^{(n)2} + b^{(n)2} + c^{(n)2} + d^{(n)2} = p$$

erhalten; das muss endlich einmal geschehen, da jede der ganzen Zahlen

$$p', p'', p''', \ldots$$

kleiner als die vorhergehende ist; p ist somit die Summe von vier Quadraten.

Zusatz. — Jede ganze Zahl ist die Summe von vier oder weniger Quadraten.

Nach No. 330 geht jede Primzahl in die Summe von vier Quadraten auf, welche prim zu einander sind; jede Primzahl ist daher die Summe von vier oder weniger Quadraten.

Da ferner jede Zahl das Produkt mehrerer Primfactoren und jeder derselben die Summe von vier Quadraten ist, so muss nach No. 245 dasselbe mit dem Produkte der Fall sein.

Satz von Legendre über das Reciprocitätsgesetz, welches zwischen zwei Primzahlen besteht.

332. Das von Legendre entdeckte Reciprocitätsgesetz besteht im folgenden Satze:

Lehrsatz. — Wenn p und q zwei beliebige ungerade Primzahlen sind, so hat man

$$\left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \left(\frac{q}{p}\right).$$

Es ist daher

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

wofern nicht p und q beide von der Form $4k + 3$ sind; in diesem letzteren Falle hat man

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Der Beweis, den wir mittheilen werden, rührt von Gauss her und ist von Legendre im zweiten Bande seiner Théorie des nombres wiederholt. Wir beweisen zunächst den folgenden Hilfssatz:

Wenn p eine positive ungerade Primzahl ist und q irgend eine durch p nicht theilbare ganze Zahl beeichnet, so liefern die Produkte

(1). $$q\,,\,2q\,,\,3q\,,\,\ldots\,,\,\frac{p-1}{2}\,q$$

$\frac{p-1}{2}$ nach dem Modul p verschiedene Reste, welche zwischen $-\frac{p-1}{2}$ und $+\frac{p-1}{2}$ liegen, und wenn die Zahl μ ausdrückt, wie viele dieser Reste negativ sind, so hat man

$$\left(\frac{q}{p}\right) = (-1)^{\mu}\,.$$

Es seien nämlich

(2). $$a_1\,,\,a_2\,,\,\ldots\,,\,a_\lambda$$

die $\lambda = \frac{p-1}{2} - \mu$ positiven und

(3). $$-b_1\,,\,-b_2\,,\,\ldots\,,\,-b_\mu$$

die μ negativen Reste.

Offenbar kann keiner der Reste Null sein; ferner können in keiner der Reihen (2) und (3) zwei gleiche Reste vorkommen; wir behaupten aber auch noch, dass a_m nicht $= b_n$ sein kann. Sind nämlich αq, βq die Vielfachen von q, welche die Reste a_m und $-b_n$ geliefert haben, so würde die Annahme $a_m = b_n$

$$\alpha q \equiv -\beta q \text{ oder } (\alpha+\beta)\,q \equiv 0 \ (mod.\ p)$$

zur Folge haben; dies ist aber unmöglich, da q nicht durch p theilbar und die Summe $\alpha+\beta$ kleiner als p ist. Daraus geht hervor, dass die aus den Zahlen a und b gebildete Reihe dieselben Zahlen enthält, wie die Reihe

$$1\,,\,2\,,\,3\,,\,\ldots\,,\,\frac{p-1}{2}\,.$$

Da die Zahlen der Reihe (1) den in (2) und (3) enthaltenen Zahlen beziehungsweise congruent sind, so ist das Produkt der einen dem Produkte der andern congruent, also

$$\left(1\,.\,2\,.\,3\,\ldots\,\frac{p-1}{2}\right) q^{\frac{p-1}{2}} \equiv (-1)^{\mu}\, a_1 a_2 \ldots a_\lambda b_1 b_2 \ldots b_\mu \ (mod.\ p).$$

Werden die Glieder dieser Congruenz beziehungsweise durch die Produkte

$$1\,.\,2\,.\,3\,\ldots\,\frac{p-1}{2}\,,\ a_1\,a_2\,\ldots\,a_\lambda\ b_1\ b_2\,\ldots\,b_\mu,$$

von deren Gleichheit wir uns soeben überzeugt haben, dividirt, so erhält man

$$q^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod{p},$$

oder

(4). $$\left(\frac{q}{p}\right) = (-1)^\mu,$$

und dies ist das Resultat, dessen Herleitung uns oblag.

Es ist jetzt leicht, einen analytischen Ausdruck der Zahl μ zu finden. Wir bezeichnen in der Folge die grösste in irgend einer Grösse x enthaltene ganze Zahl mit $E(x)$, so dass die Differenz $x - E(x)$ positiv und kleiner als 1 ist. Dies vorausgesetzt, seien αq und βq die Produkte, welche die Reste a und $-b$ liefern; dann ist

$$\frac{\alpha q}{p} = E\left(\frac{\alpha q}{p}\right) + \frac{a}{p}, \quad \frac{\beta q}{p} = E\left(\frac{\beta q}{p}\right) + \frac{p-b}{p},$$

oder, wenn mit 2 multiplicirt wird,

$$\frac{2\alpha q}{p} = 2\,E\left(\frac{\alpha q}{p}\right) + \frac{2a}{p}, \quad \frac{2\beta q}{p} = 2\,E\left(\frac{\beta q}{p}\right) + 1 + \frac{p-2b}{p}.$$

Da $2a$ und $2b$ kleiner als p sind, so sind

$$2\,E\left(\frac{\alpha q}{p}\right) \text{ und } 2\,E\left(\frac{\beta q}{p}\right) + 1$$

die grössten beziehungsweise in $\frac{2\alpha q}{p}$ und $\frac{2\beta q}{p}$ enthaltenen ganzen Zahlen; man hat daher

$$E\left(\frac{2\alpha q}{p}\right) - 2\,E\left(\frac{\alpha q}{p}\right) = 0,$$

$$E\left(\frac{2\beta q}{p}\right) - 2\,E\left(\frac{\beta q}{p}\right) = 1.$$

Ertheilen wir α und β alle Werthe, welche diese Zahlen annehmen können, so liefern die vorhergehenden Formeln $\lambda + \mu$ verschiedene Gleichungen, durch deren Addition sich ergiebt:

$$\mu = E\left(\frac{2q}{p}\right) + E\left(\frac{4q}{p}\right) + \cdots + E\left[\frac{(p-3)q}{p}\right] + E\left[\frac{(p-1)q}{p}\right]$$
$$- 2\,E\left(\frac{q}{p}\right) - 2\,E\left(\frac{2q}{p}\right) - \cdots - 2\,E\left(\frac{p-1}{2}\cdot\frac{q}{p}\right).$$

In dieser Formel können die Terme der zweiten Reihe sämmtlich unterdrückt werden, da dieselben gerade Zahlen sind und wir überhaupt nur wissen wollen, ob μ eine gerade oder eine ungerade Zahl ist. Wir schreiben aus diesem Grunde einfach

$$(5).\quad \left.\begin{cases} \mu \equiv E\left(\frac{2q}{p}\right) + E\left(\frac{4q}{p}\right) + \cdots \\ \quad + E\left[\frac{(p-3)q}{p}\right] + E\left[\frac{(p-1)q}{p}\right] \end{cases}\right\} (mod.\ 2).$$

Setzt man

$$\frac{nq}{p} = E\left(\frac{nq}{p}\right) + \vartheta$$

und subtrahirt jedes Glied dieser Formel von q, so erhält man

$$\frac{(p-n)q}{p} = (q-1) - E\left(\frac{nq}{p}\right) + (1-\vartheta);$$

es ist daher für jeden Werth von n

$$E\left[\frac{(p-n)q}{p}\right] = (q-1) - E\left(\frac{nq}{p}\right).$$

Wird zum zweiten Gliede die gerade Zahl $2\,E\left(\frac{nq}{p}\right)$ addirt, so folgt

$$(6).\quad E\left[\frac{(p-n)q}{p}\right] \equiv (q-1) + E\left(\frac{nq}{p}\right) (mod.\ 2).$$

Wir setzen jetzt $p = 4i \pm 1$ und lassen n die Werthe 1, 3, 5, ..., $(2i-1)$ annehmen; mit Rücksicht auf die so erhaltenen Resultate geht die Congruenz (5) über in

$$(7).\quad \left.\begin{cases} \mu \equiv i\,(q-1) + E\left(\frac{q}{p}\right) + E\left(\frac{2q}{p}\right) + E\left(\frac{3q}{p}\right) + \cdots \\ \quad + E\left(\frac{p-1}{2}\cdot\frac{q}{p}\right) \end{cases}\right\} (mod.2).$$

Diese Formel (7) besteht für jeden Werth der Zahl q, wenn dieselbe nur nicht durch p theilbar ist, eine Bemerkung, die uns später von Nutzen sein wird. Ist q ungerade, also $q-1$ gerade, so reducirt sich die Congruenz (7) auf

$$(8).\quad \left.\begin{cases} \mu \equiv E\left(\frac{q}{p}\right) + E\left(\frac{2q}{p}\right) + E\left(\frac{3q}{p}\right) + \cdots \\ \quad + E\left(\frac{p-1}{2}\cdot\frac{q}{p}\right) \end{cases}\right\} (mod.\ 2),$$

und dieser Werth lässt sich, wie wir sehen werden, auf eine andere Form bringen. Wir setzen in der Folge $q < p$ voraus; dann ist der erste Term des zweiten Gliedes der Formel (8) Null, und der letzte Term hat den Werth $\frac{q-1}{2}$; denn es ist

$$\frac{p-1}{2} \cdot \frac{q}{p} = \frac{q-1}{2} + \frac{p-q}{2p} .$$

Es sei nun n eine gegebene ganze Zahl, die $=$ oder $< \frac{q-1}{2}$ ist, und es bezeichne m die Anzahl der Terme des vorstehenden Werthes von μ, welche kleiner als n sind. Da die Zahl $m+1$ kleiner als p ist, so kann der Ausdruck $\frac{(m+1)q}{p}$ sich nie auf eine ganze Zahl reduciren, und man hat folglich:

$$E\left(\frac{mq}{p}\right) < n \ , \ E\left[\frac{(m+1)q}{p}\right] > n \, ,$$

woraus sich

$$\frac{mq}{p} < n \ , \ \frac{(m+1)q}{p} > n \, ,$$

oder

$$m < \frac{np}{q} < m+1$$

ergiebt. Diese Ungleichungen drücken aus, dass m die grösste in $\frac{np}{q}$ enthaltene ganze Zahl ist; man hat also

$$m = E\left(\frac{np}{q}\right) .$$

Ebenso enthält das zweite Glied der Formel (8)

$$E\left[\frac{(n+1)p}{q}\right]$$

Terme, welche kleiner als $n+1$ sind, wenn $n+1$ nicht grösser als $\frac{q-1}{2}$, d. h. wenn

$$n < \frac{q-1}{2}$$

ist. Unter dieser Voraussetzung enthält danach unser Ausdruck von μ

$$E\left[\frac{(n+1)p}{q}\right] - E\left(\frac{np}{q}\right) \tag{9}$$

Terme, die gleich n sind. Ausserdem ist die Gesammtzahl der Terme des Ausdrucks von μ $\frac{p-1}{2}$ und da

$$E\left(\frac{q-1}{2} \cdot \frac{p}{q}\right)$$

dieser Terme kleiner als $\frac{q-1}{2}$ sind, so sind

$$(10).\qquad \frac{p-1}{2} - E\left(\frac{q-1}{2}\cdot\frac{p}{q}\right)$$

Terme von μ gleich $\frac{q-1}{2}$.

Multiplicirt man den Ausdruck (9) mit n, ersetzt darauf n durch jeden der Werthe

$$1, 2, 3, \ldots, \left(\frac{p-1}{2} - 1\right),$$

und addirt alle Resultate zu dem Produkte des Ausdrucks (10) in $\frac{q-1}{2}$, so wird man offenbar wieder den Werth von μ erhalten. Es ist daher

$$\left.\begin{aligned}\mu \equiv\ & \left[E\left(\frac{2p}{q}\right) - E\left(\frac{p}{q}\right)\right]\\ & + 2\left[E\left(\frac{3p}{q}\right) - E\left(\frac{2p}{q}\right)\right]\\ & + \ldots\ldots\ldots\ldots\\ & + \frac{q-3}{2}\left[E\left(\frac{q-1}{2}\cdot\frac{p}{q}\right) - E\left(\frac{q-3}{2}\cdot\frac{p}{q}\right)\right]\\ & + \frac{q-1}{2}\left[\frac{p-1}{2} - E\left(\frac{q-1}{2}\cdot\frac{p}{q}\right)\right]\end{aligned}\right\}(mod.\ 2),$$

oder einfacher

$$(11).\quad \mu \equiv \frac{p-1}{2}\cdot\frac{q-1}{2} - \left[E\left(\frac{p}{q}\right) + E\left(\frac{2p}{q}\right) + \cdots + E\left(\frac{q-1}{2}\cdot\frac{p}{q}\right)\right] (mod. 2).$$

Bei der Herleitung der Formel (8) wurde vorausgesetzt, dass p eine ungerade Primzahl und q irgend eine ungerade Zahl sei. Nehmen wir also an, q sei eine Primzahl, und machen

$$(12).\qquad \left(\frac{p}{q}\right) = (-1)^{\nu},$$

so wird die Zahl ν durch die Formel (8) bestimmt, wenn darin die Buchstaben p und q gegen einander vertauscht werden; man erhält auf diese Weise

$$(13).\quad \nu \equiv E\left(\frac{p}{q}\right) + E\left(\frac{2p}{q}\right) + \cdots + E\left(\frac{q-1}{2}\cdot\frac{p}{q}\right)\ (mod.\ 2).$$

Der Vergleich der Formeln (11) und (13) liefert:

$$\mu + \nu \equiv \frac{p-1}{2}\cdot\frac{q-1}{2}\ (mod.\ 2);$$

ausserdem hat man den Formeln (4) und (12) zufolge

$$\left(\frac{q}{p}\right) = (-1)^{\mu+\nu}\left(\frac{p}{q}\right),$$

mithin

(14). $$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right);$$

und dies ist die Formel, welche wir herleiten wollten.

Anmerkung. — Es ist zu beachten, dass die Zahl -1 Rest aller Primzahlen $4i+1$, aber Nichtrest aller Primzahlen $4i+3$ ist.

Der in No. 311 gegebenen Definition gemäss ist nämlich

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Dies ergiebt sich übrigens auch aus unserer Formel (8); denn für $q = -1$ reducirt sich jeder Term des zweiten Gliedes dieser Formel auf -1, und man hat

$$\mu \equiv -\frac{p-1}{2} \equiv \frac{p-1}{2} \pmod{2}.$$

Daraus geht hervor, dass die Congruenz

$$x^2 + 1 \equiv 0 \pmod{p}$$

möglich oder unmöglich ist, je nachdem p die Form $4i+1$ oder $4i+3$ hat. Findet der erste Fall statt, so geht p in die Summe zweier Quadrate auf und ist folglich selbst die Summe zweier Quadrate, zu welchem Resultate uns bereits der Wilson'sche Satz geführt hat.

333. Die Formel (7) der vorhergehenden Nummer setzt, wie wir oben bemerkt haben, nur voraus, dass q nicht durch p theilbar ist. Nehmen wir $q = 2$ an, so reduciren sich die in (7) vorkommenden Ausdrücke $E\left(\frac{q}{p}\right)$, ... sämmtlich auf Null, und man erhält

$$\mu \equiv i \equiv \frac{p \mp 1}{4} \pmod{2};$$

ausserdem ist $\frac{p \pm 1}{2}$ eine ungerade Zahl, und man kann schreiben

$$\mu \equiv \frac{(p+1)(p-1)}{8} \pmod{2}.$$

Setzt man zweitens $q = -2$, so reduciren sich die Ausdrücke

$$E\left(\frac{q}{p}\right),\ E\left(\frac{2q}{p}\right), \dots$$

der Formel (7) sämmtlich auf -1, und man erhält

$$\mu \equiv i - \frac{p-1}{2} \equiv \frac{(p+1)(p-1)}{8} - \frac{p-1}{2} \ (mod.\ 2),$$

oder

$$\mu \equiv \frac{(p-1)(p-3)}{8} \ (mod.\ 2).$$

Für jede ungerade Primzahl p ist danach

$$\left(\frac{2}{p}\right) = (-1)^{\frac{(p+1)(p-1)}{8}}, \quad \left(\frac{-2}{p}\right) = (-1)^{\frac{(p-1)(p-3)}{8}},$$

und diese Formeln enthalten den folgenden Satz:

Lehrsatz. — Die Zahl $+2$ ist quadratischer Rest jeder Primzahl von einer der beiden Formen $8k+1$, $8k+7$; sie ist Nichtrest jeder Primzahl von einer der beiden Formen $8k+3$, $8k+5$.

Die Zahl -2 ist quadratischer Rest jeder Primzahl von einer der beiden Formen $8k+1$, $8k+3$; sie ist Nichtrest jeder Primzahl von einer der beiden Formen $8k+5$, $8k+7$.

334. Es dürfte von Nutzen sein, einige Anwendungen des Satzes von Legendre hier folgen zu lassen.

Für die Primzahlen 3 und $p = 3n \pm 1$ ist

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{\pm 1}{3}\right);$$

ausserdem ist $+1$ Rest, -1 Nichtrest von 3. Theilt man daher die Primzahlen in die vier Klassen:

$$12k+1, \quad 12k+5, \quad 12k+7, \quad 12k+11,$$

so erhält man den Satz:

Die Zahl $+3$ ist quadratischer Rest aller Primzahlen $12k+1$ und $12k+11$, Nichtrest aller Primzahlen $12k+5$ und $12k+7$.

Mit Rücksicht auf die Bemerkungen, die wir in No. 311 machten, können wir hinzufügen:

Die Zahl -3 ist Rest aller Primzahlen $12k+1$, $12k+7$, Nichtrest aller Primzahlen $12k+5$, $12k+11$.

Diese beiden Sätze sind zuerst von Euler im 8ten Bande der Comment. nov. Petrop. bewiesen.

Hinsichtlich der Primzahlen 5 und p hat man

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right);$$

es ist aber

$$\left(\frac{p}{5}\right) = \pm 1,$$

je nachdem p von der Form $5n \pm 1$ oder von der Form $5n \pm 2$ ist. Theilt man daher die Primzahlen nach dem Rest, der sich bei ihrer Division durch 20 ergiebt, in die acht Klassen

$$20k + 1\,,\ 20k + 3\,,\ 20k + 7\,,\ 20k + 9$$
$$20k + 11,\ 20k + 13,\ 20k + 17,\ 20k + 19,$$

so erhält man folgenden Satz:

Die Zahl $+5$ ist quadratischer Rest aller Primzahlen einer der Formen

$$20k + 1\,,\ 20k + 9\,,\ 20k + 11\,,\ 20k + 19;$$

sie ist Nichtrest aller Primzahlen der Formen

$$20k + 3\,,\ 20k + 7\,,\ 20k + 13\,,\ 20k + 17.$$

Die Zahl -5 ist quadratischer Rest aller Primzahlen der Formen

$$20k + 1\,,\ 20k + 3\,,\ 20k + 7\,,\ 20k + 9;$$

sie ist Nichtrest aller Primzahlen der Formen

$$20k + 11\,,\ 20k + 13\,,\ 20k + 17\,,\ 20k + 19.$$

Ueber die Congruenz $x^2 - N \equiv 0$ (*mod.* p), deren Modul p eine Primzahl ist.

335. Der Satz von Legendre liefert das Mittel, durch eine leichte Rechnung zu entscheiden, ob die Congruenz

$$x^2 - N \equiv 0 \ (mod.\ p)$$

lösbar ist oder nicht; denn die Bedingung, unter welcher dieser Congruenz genügt werden kann, ist

$$\left(\frac{N}{p}\right) = +1.$$

Es kommt also nur darauf an, das Zeichen des Symbols $\left(\frac{N}{p}\right)$ zu bestimmen. Die Zahl N kann immer unter p hinabgedrückt werden; hat man dann

$$N = a^\alpha\, b^\beta\, c^\gamma \ldots,$$

wo $a, b, c, \ldots$ ungleiche Primfactoren bezeichnen, so ist

$$\left(\frac{N}{p}\right) = \left(\frac{a^\alpha}{p}\right)\left(\frac{b^\beta}{p}\right)\left(\frac{c^\gamma}{p}\right)\ldots;$$

nun ist offenbar

$$\left(\frac{a^\alpha}{p}\right) = +1,$$

wenn α gerade, und

$$\left(\frac{a^\alpha}{p}\right) = \left(\frac{a}{p}\right),$$

wenn α ungerade ist. Die Bestimmung von $\left(\frac{N}{p}\right)$ ist daher auf diejenige der einfacheren Symbole

$$\left(\frac{a}{p}\right), \left(\frac{b}{p}\right), \ldots$$

zurückgeführt; $a, b, \ldots$ sind die Primfactoren von N, welche in dieser Zahl mit ungeraden Exponenten versehen sind.

Betrachten wir eins dieser Symbole, z. B. $\left(\frac{a}{p}\right)$. Sein Werth ist unmittelbar bekannt, wenn $a = 2$ ist. Im entgegengesetzten Falle wird die Bestimmung von $\left(\frac{a}{p}\right)$ durch den Satz von Legendre auf diejenige von $\left(\frac{p}{a}\right)$ zurückgeführt. Verfährt man dann mit $\left(\frac{p}{a}\right)$ ebenso, wie wir mit $\left(\frac{N}{p}\right)$ verfuhren, u. s. w., so wird man jedenfalls zu Symbolen gelangen, deren Werth bekannt ist.

Beispiel. — Wir wollen eine der von Legendre in seiner Théorie des nombres betrachteten Congruenzen, nämlich

$$x^2 + 1459 \equiv 0 \ (mod.\ 22366891)$$

untersuchen.

Der Modul ist eine Primzahl $4k + 3$, und auch 1459 ist eine Primzahl dieser Form; man hat daher

$$\left(\frac{N}{p}\right) = \left(\frac{-1459}{22366891}\right) = -\left(\frac{1459}{22366891}\right) = \left(\frac{22366891}{1459}\right).$$

Der Rest der Division von 22366891 durch 1459 ist 421, mithin

$$\left(\frac{N}{p}\right) = \left(\frac{421}{1459}\right).$$

421 ist eine Primzahl von der Form $4k + 1$, folglich

$$\left(\frac{N}{p}\right) = \left(\frac{1459}{421}\right) = \left(\frac{196}{421}\right) = \left(\frac{4 \times 49}{421}\right) = 1,$$

da 4×49 ein Quadrat ist.

Die vorgelegte Congruenz besitzt daher zwei Wurzeln.

336. Nachdem man erkannt hat, dass die Congruenz

$$x^2 - N \equiv 0 \ (mod.\ p)$$

möglich ist, handelt es sich darum, sie aufzulösen. Wir unterscheiden dabei zwei Fälle, je nachdem der Modul p von der Form $4k+3$, oder von der Form $4k+1$ ist.

Es sei zunächst

$$p = 4k + 3;$$

wenn die vorgelegte Congruenz möglich ist, so hat man

$$N^{\frac{p-1}{2}} - 1 \equiv 0 \text{ oder } N^{2k+1} - 1 \equiv 0 \ (mod.\ p),$$

oder auch

$$N^{2k+2} - N \equiv 0 \ (mod.\ p).$$

Daraus folgt, dass die Wurzeln unserer Congruenz folgende sind:

$$x \equiv \pm N^{k+1}.$$

Es sei jetzt p von der Form $4k+1$. Die Zahlen $4k+1$ zerfallen in zwei Arten, in Zahlen von der Form $8k+1$ und in solche von der Form $8k+5$; wir werden jede Art für sich betrachten.

Wird

$$p = 8k + 5$$

vorausgesetzt, so hat man, wenn die vorgelegte Congruenz möglich ist,

$$N^{4k+2} - 1 \equiv 0 \ (mod.\ p),$$

oder

$$(N^{2k+1} + 1)\ (N^{2k+1} - 1) \equiv 0 \ (mod.\ p).$$

Es ist daher entweder

$$N^{2k+1} - 1 \equiv 0 \ (mod.\ p),$$

oder

$$N^{2k+1} + 1 \equiv 0 \ (mod.\ p).$$

Wenn der erste dieser beiden Fälle stattfindet, so ergiebt sich

$$N^{2k+2} - N \equiv 0 \ (mod.\ p),$$

und folglich hat die vorgelegte Congruenz die Wurzeln

$$x \equiv \pm N^{k+1} \ (mod.\ p).$$

Findet dagegen der zweite Fall statt, so setzen wir

$$\vartheta \equiv N^{k+1} \ (mod.\ p), \text{ so dass } \vartheta^2 \equiv N^{2k+2} \equiv -N \ (mod.\ p)$$

ist; dann geht die vorgelegte Congruenz über in

$$x^2 + \vartheta^2 \equiv 0 \ (mod.\ p).$$

Nun hat p die Form $4k + 1$; man kann daher p als Summe zweier Quadrate darstellen, die prim zu einander sind. Ist

$$p = \alpha^2 + \beta^2,$$

und bezeichnen t und u zwei unbestimmte Grössen, so folgt

$$(\alpha^2 + \beta^2)(t^2 + u^2) = (\alpha t + \beta u)^2 + (\alpha u - \beta t)^2 \equiv 0 \ (mod.\ p).$$

Bestimmt man jetzt t und u mittels der Bedingung

$$\alpha u - \beta t = \vartheta,$$

so liegt auf der Hand, dass die vorgelegte Congruenz durch die Werthe

$$x \equiv \pm (\alpha t + \beta u) \ (mod.\ p)$$

befriedigt wird.

Wir haben jetzt noch den Fall zu untersuchen, in welchem p die Form $8k + 1$ hat. Dann ist es im Allgemeinen nicht möglich, die vorgelegte Congruenz ohne Versuche zu lösen, und man ist genöthigt, die Terme der Reihe

$$p + N, \ 2p + N, \ 3p + N, \ldots$$

zu berechnen, bis man zu einem Term gelangt, welcher ein vollständiges Quadrat ist. Dies wird nothwendig einmal geschehen, wenn die vorgelegte Congruenz möglich ist, und da das gesuchte Quadrat kleiner als $\frac{1}{4} p^2$ ist, so kann die Anzahl der Terme der vorstehenden Reihe, die man zu berechnen hat, nie grösser als $\frac{1}{4} p$ sein.

Es kann in dem vorliegenden Falle aber auch vorkommen, dass sich die gesuchten Wurzeln direkt bestimmen lassen. Es sei nämlich 2^μ die höchste in $p - 1$ enthaltene Potenz von 2, und es werde

$$p = 2^\mu \alpha + 1$$

gesetzt; α ist eine ungerade Zahl und μ wenigstens gleich 3. Da die vorgelegte Congruenz möglich ist, so hat man

$$N^{2^{\mu-1}\alpha} \equiv 1 \ (mod.\ p),$$

und es ist möglicherweise auch

$$N^\alpha \equiv \pm 1 \ (mod.\ p).$$

Unter dieser Voraussetzung ist

$$N^{\alpha+1} \equiv \pm N \pmod{p},$$

und da α ungerade ist, so können wir ganz ebenso verfahren, wie es im Falle $p = 8k + 5$ geschah.

Ueber die Congruenz $x^2 - N \equiv 0$, wenn der Modul eine beliebige Zahl ist.

337. Wir nehmen zunächst an, der Modul sei eine Potenz p^ν einer ungeraden Primzahl p, es sei also die Congruenz

$$(1). \qquad x^2 - N \equiv 0 \pmod{p^\nu}$$

vorgelegt. Wir lösen diese Congruenz zuerst in Beziehung auf den Modul p und bezeichnen ihre Wurzeln, welche sich durch Anwendung der in No. 336 dargelegten Methode ergeben, mit $\pm \xi$; dann ist

$$(2). \qquad \xi^2 - N \equiv 0 \pmod{p},$$

und folglich

$$(\xi^2 - N)^\nu \equiv 0 \pmod{p^\nu}.$$

Nun erhält man durch Entwicklung der Potenz $(\xi + \sqrt{N})^\nu$ ein Resultat von der Form

$$(3). \qquad (\xi + \sqrt{N})^\nu = \alpha + \beta \sqrt{N},$$

worin α und β ganze Zahlen sind; daraus ergiebt sich

$$(4). \qquad (\xi - \sqrt{N})^\nu = \alpha - \beta \sqrt{N},$$

also ist

$$(5). \qquad \alpha^2 - N\beta^2 = (\xi^2 - N)^\nu \equiv 0 \pmod{p^\nu}.$$

Die Formel (3) oder (4) liefert auch

$$\alpha = \xi^\nu + \frac{\nu(\nu-1)}{1 \cdot 2} \xi^{\nu-2} N + \cdots,$$

$$\beta = \frac{\nu}{1} \xi^{\nu-1} + \frac{\nu(\nu-1)(\nu-2)}{1 \cdot 2 \cdot 3} \xi^{\nu-3} N + \cdots,$$

oder, der Formel (2) wegen,

$$\alpha \equiv \xi^\nu \left[1 + \frac{\nu(\nu-1)}{1 \cdot 2} + \cdots\right] \equiv 2^{\nu-1} \xi^\nu \pmod{p},$$

$$\beta \equiv \xi^{\nu-1} \left[\frac{\nu}{1} + \frac{\nu(\nu-1)(\nu-2)}{1 \cdot 2 \cdot 3} + \cdots\right] \equiv 2^{\nu-1} \xi^{\nu-1} \pmod{p},$$

woraus hervorgeht, dass p weder in α noch in β aufgehen kann. Dann lassen sich zwei ganze Zahlen t und u von solcher Beschaffenheit ermitteln, dass man

(6). $$\alpha = \beta t + p^\nu u$$

hat, und wenn dieser Werth von α in die Formel (5) eingesetzt wird, so folgt

$$\beta^2 (t^2 - N) \equiv 0 \ (mod. \ p^\nu),$$

oder

(7). $$t^2 - N \equiv 0 \ (mod. \ p^\nu);$$

demnach hat die vorgelegte Congruenz die beiden Wurzeln

$$x = \pm t.$$

Anmerkung. — Wir haben bisher den Fall ausgeschlossen, in welchem die Zahl N ein Vielfaches von p ist; dann fordert die vorgelegte Congruenz, dass auch x durch p theilbar sei. Ist $N = p^{2n} N'$, wo n den Grad der höchsten in N aufgehenden Potenz von p^2 bezeichnet, so kann der vorgelegten Congruenz nur unter der Bedingung genügt werden, dass x theilbar ist durch p^n. Setzt man nun $x = p^n z$, so reducirt sich die Congruenz auf

$$z^2 - N' \equiv 0 \ (mod. \ p^{\nu - 2n}),$$

und diese ist unmöglich oder hat nur die Wurzel $z = 0$, wenn auch N' noch den Factor p enthält.

338. Wir betrachten ferner die Congruenz

$$x^2 - N \equiv 0 \ (mod. \ 2^\nu).$$

Ist 2^{2n} die höchste in N aufgehende Potenz von 2^2, so muss x offenbar durch 2^n theilbar sein, und wenn

$$N = 2^{2n} N', \ x = 2^n z$$

gesetzt wird, so geht unsere Congruenz über in

$$z^2 - N' \equiv 0 \ (mod. \ 2^{\nu - 2n}).$$

Man kann danach N als ungerade oder als das Doppelte einer ungeraden Zahl voraussetzen. Ist N das Doppelte einer ungeraden Zahl, so kann die vorgelegte Congruenz offenbar nur dann gelöst werden, wenn $\nu = 1$ ist; von diesem Falle dürfen wir abstrahiren.

Es sei also N eine ungerade Zahl. Für $\nu = 2$ reducirt sich die vorgelegte Congruenz auf

$$x^2 - 1 \equiv 0 \text{ oder auf } x^2 + 1 \equiv 0 \ (mod. \ 4);$$

nur die erstere dieser Congruenzen ist möglich und hat die Wurzeln ± 1.

Wenn $\nu > 2$ ist, so ist die vorgelegte Congruenz unmöglich, wofern nicht N die Form $8k + 1$ hat, und man erhält leicht eine Lösung durch successive Substitutionen. Es ist zu beachten, dass eine besondere Lösung zur allgemeinen führt. Bezeichnet nämlich x_0 eine Wurzel der vorgelegten Congruenz, so lässt sich dieselbe auf die Form

$$(x - x_0)\,(x + x_0) \equiv 0 \;(mod.\; 2^\nu)$$

bringen; daraus folgt

$$x \pm x_0 = 2t\;,\; x \mp x_0 = 2^{\nu-1}\,u,$$

wo t und u unbestimmte Grössen sind. Es ist danach

$$t = 2^{\nu-2}\,u \pm x_0;$$

u ist willkürlich, und die gesuchten Wurzeln sind durch folgende Formel gegeben:

$$x \equiv \pm x_0 + 2^{\nu-1}\,u \;(mod.\; 2^\nu).$$

Beispiel. — Es soll die Congruenz

$$x^2 + 15 \equiv 0 \;(mod.\; 2^{10})$$

gelöst werden. Der Werth $x = 1$ genügt derselben, wenn 2^4 statt 2^{10} zum Modul genommen wird; man macht deshalb

$$x = 1 + 8\,x_1$$

und erhält durch Einsetzung dieses Werthes in die vorgelegte Congruenz

$$1 + x_1 + 4\,x_1^{\,2} \equiv 0 \;(mod.\; 2^6).$$

Daraus ist ersichtlich, dass $1 + x_1$ durch 4 theilbar sein muss; man wird daher

$$x_1 = -\,1 + 4\,x_2$$

machen; dadurch ergiebt sich

$$1 - 7\,x_2 + 16\,x_2^{\,2} \equiv 0 \;(mod.\; 2^4),$$

oder

$$1 - 7\,x_2 \equiv 0 \;(mod.\; 2^4).$$

Dies ist eine Congruenz ersten Grades; ihre Wurzel ist 7, und, wenn

$$x_2 = 7$$

gemacht wird, so erhält man $x_1 = 27$, $x = 217$. Die Wurzeln der vorgelegten Congruenz sind also durch die Formel

$$x = \pm 217 + 512\,u$$

bestimmt, welche die vier Zahlen

$$217\;,\;295\;,\;729\;,\;807$$

umfasst.

339. Der Fall, in welchem der Modul M der vorgelegten Congruenz

$$x^2 - N \equiv 0 \;(mod.\; M)$$

eine beliebig zusammengesetzte Zahl ist, lässt sich mittels eines schon einmal angewandten Schlussverfahrens auf die früheren Fälle zurückführen. Es sei

$$M = p^\nu\, q^\mu\, r^\lambda \ldots,$$

wo $p, q, r, \ldots$ ungleiche Primzahlen bezeichnen. Jede Zahl, welche der vorstehenden Congruenz nach dem Modul M genügt, muss ihr auch in Beziehung auf die Moduln p^ν, q^μ, r^λ, ... genügen. Sind $a, b, c, \ldots$ beziehungsweise Wurzeln dieser Congruenzen, so erhält man, wie wir in No. 325 bei Gelegenheit eines ähnlichen Falles bemerkt haben, eine der gesuchten Lösungen dadurch, dass man die Zahl x mittels der Bedingungen

$$x \equiv a \;(mod.\; p^\nu)\;,\; x \equiv b \;(mod.\; q^\mu)\;,\; x \equiv c \;(mod.\; r^\lambda)\;,\;\ldots$$

bestimmt; diese Aufgabe hat aber bereits ihre Erledigung gefunden.

Drittes Kapitel.

Eigenschaften der ganzen Functionen einer Veränderlichen in Beziehung auf einen Primzahlmodul.

Ganze Functionen; die nach einem Primzahlmodul irreductibel sind.

340. Ich werde im Folgenden eine bereits in der vorigen Auflage dieses Werkes auseinandergesetzte wichtige Theorie mit ganz neuen Entwicklungen und von einem etwas anderen Gesichtspunkte aus vorführen. Diese Theorie bezieht sich ausschliesslich auf Primzahlmoduln; sie war der Gegenstand einer Abhandlung, die ich am 4. December 1865 der Akademie der Wissenschaften vorgelegt habe.

Es seien p eine Primzahl und $\varphi(x)$, $F(x)$ zwei ganze Functionen von x mit ganzen Coefficienten. Wenn man zwei ganze Functionen $\psi(x)$, $\chi(x)$ mit ganzen Coefficienten ermitteln kann, die von solcher Beschaffenheit sind, dass man identisch

$$\varphi(x)\ \psi(x) = F(x) + p\chi(x),$$

folglich

$$\varphi(x)\,\psi(x) \equiv F(x) \pmod{p}$$

hat, so sagen wir, die Function $F(x)$ sei durch $\varphi(x)$ in Beziehung auf den Modul p theilbar, oder sie sei nach dem Modul p gleich dem Produkte der Functionen $\varphi(x)$, $\psi(x)$.

Setzen wir voraus, eine ganze Function $\varphi(x)$ sei nach abnehmenden Potenzen von x geordnet. Wenn alle Coefficienten durch p theilbar sind, so ist die Function Null in Beziehung auf den Modul p. Im entgegengesetzten Falle sei a der erste in Beziehung auf p von Null verschiedene Coefficient; dann lässt sich eine ganze Zahl α ermitteln, für welche

$$a\alpha \equiv 1 \pmod{p}$$

ist, und folglich kann man das Produkt $\alpha\varphi(x)$ auf die Form

$$\alpha\varphi(x) = F(x) + p\chi(x)$$

bringen, worin $F(x)$ eine ganze Function bezeichnet, deren höchster Term den Coefficienten Eins hat; man darf offenbar voraussetzen, alle übrigen Coefficienten seien unter p hinabgedrückt.

Eine ganze Function $F(x)$ mit ganzen Coefficienten soll irreductibel in Beziehung auf den Primzahlmodul p heissen, wenn sie in Beziehung auf diesen Modul durch keine ganze Function theilbar ist, deren Grad kleiner als der ihrige ist, und wenn ausserdem die höchste in ihr enthaltene Potenz von x den Coefficienten Eins hat.

341. Lehrsatz I. — Wenn die beiden Functionen $\varphi(x)$ und $\psi(x)$ in Beziehung auf den Primzahlmodul p keinen gemeinschaftlichen Divisor besitzen, so lassen sich zwei ganze Functionen U und V von der Beschaffenheit ermitteln, dass identisch

$$U\varphi(x) - V\psi(x) \equiv 1 \pmod{p}$$

ist.

Bezeichnen a und b die Coefficienten der höchsten Potenz von x in $\varphi(x)$ und in $\psi(x)$, so kann man

$$\varphi(x) \equiv aA\,,\quad \psi(x) \equiv bB \pmod{p}$$

setzen, wo A und B ganze Functionen von x sind, in welchen die höchste Potenz von x den Coefficienten Eins hat.

Dies vorausgesetzt, verfahren wir mit den Polynomen A und B in der Weise, als wollten wir ihren grössten gemeinschaftlichen Divisor bestimmen. Dabei vernachlässigen wir die mit p multiplicirten Terme und fügen jedem Rest ein Polynom von der Form $p\cdot\lambda(x)$ hinzu, welches so gewählt ist, dass der fragliche Rest nach dieser Addition durch den Coefficienten des höchsten Terms theilbar ist. Ausserdem haben wir, bevor wir diesen Rest als Divisor benutzen, den allen seinen Termen gemeinschaftlichen Factor zu unterdrücken. Da wir voraussetzen, dass die Polynome A und B keinen gemeinschaftlichen Divisor besitzen, so muss diese Operation zu einem numerischen Rest r_n führen, welcher nach dem Modul p nicht Null sein kann, und wenn wir noch, um in dieser Beziehung überhaupt eine Bestimmung zu treffen, annehmen, dass der Grad von B nicht kleiner als derjenige von A ist, so erhalten wir folgende Reihe von Congruenzen:

$$\left.\begin{array}{lll} A & \equiv B & Q_1 + r_1 R_1 \\ B & \equiv R_1 & Q_2 + r_2 R_2 \\ R_1 & \equiv R_2 & Q_3 + r_3 R_3 \\ \cdots & \cdots & \cdots \\ R_{n-2} & \equiv R_{n-1} & Q_n + r_n \end{array}\right\} (mod.\ p);$$

$r_1, r_2, \ldots, r_n$ sind ganze Zahlen, die nach dem Modul p nicht Null sein können, und $R_1, R_2, \ldots, Q_1, Q_2, \ldots$ sind ganze Functionen von x, in welchen die höchste Potenz von x den Coefficienten 1 hat. Aus diesen Relationen ergiebt sich

$$\left.\begin{array}{l} r_1 R_1 \equiv A - Q_1 B \\ r_1 r_2 R_2 \equiv (r_1 + Q_1 Q_2) B - Q_2 A \\ r_1 r_2 r_3 R_3 \equiv (r_2 + Q_2 Q_3) A - [r_2 Q_1 + (r_1 + Q_1 Q_2) Q_3] B \\ \cdots\cdots\cdots\cdots \end{array}\right\} (mod.\ p).$$

Die letzte der Congruenzen, die auf diese Weise entstehen, hat offenbar die Form

$$r_1 r_2 \ldots r_n \equiv MA - NB \ (mod.\ p),$$

und darin sind M und N ganze Functionen. Es sei nun α die Zahl, mit welcher man das Produkt $a\, b\, r_1 r_2 \ldots r_n$ multipliciren muss, damit das Resultat nach dem Modul p der Einheit congruent sei; wird dann die letzte Congruenz mit $a b \alpha$ multiplicirt und U statt $b \alpha M$, V statt $a \alpha N$ geschrieben, so folgt

$$1 \equiv U\varphi(x) - V\psi(x) \ (mod.\ p),$$

oder

$$1 + p\chi(x) = U\varphi(x) - V\psi(x),$$

w. z. b. w.

342. Lehrsatz II. — Wenn die ganze Function $F(x)$, welche nach dem Primzahlmodul p irreductibel ist, in Beziehung auf diesen Modul in das Produkt $\varphi(x)\ \psi(x)$ der ganzen Functionen $\varphi(x)$ und $\psi(x)$ aufgeht, so geht sie in wenigstens einen der beiden Factoren auf.

Wenn nämlich $\psi(x)$ in Beziehung auf den Modul p nicht durch $F(x)$ theilbar ist, so besitzt $F(x)$, als irreductibele Function, keinen einzigen der Divisoren, welche $\psi(x)$ enthalten kann. Es lassen sich daher drei ganze Functionen P, U und V von der Beschaffenheit ermitteln, dass

$$1 + pP = UF(x) - V\psi(x)$$

ist. Ausserdem hat man der Voraussetzung nach

$$\varphi(x)\,\psi(x) - F(x)\,f(x) = p\,\chi(x),$$

worin $f(x)$ und $\chi(x)$ ganze Functionen bezeichnen, und durch Multiplication dieser beiden Gleichungen erhält man

$$[\varphi(x)\,\psi(x) - F(x)\,f(x)]\,(1 + pP) = p\chi(x)\,[UF(x) - V\psi(x)],$$

oder

$$\psi(x)\left\{\varphi(x) + p[P\varphi(x) + V\chi(x)]\right\} = F(x)\,\left\{f(x) + p[Pf(x) + U\chi(x)]\right\}.$$

Das Polynom $F(x)$ geht daher algebraisch in das erste Glied der vorhergehenden Formel auf. Da nun, wie wir eben gesehen haben, $F(x)$ mit $\psi(x)$ keinen Factor gemeinschaftlich hat, so muss die Function

$$\varphi(x) + p\,[P\varphi(x) + V\chi(x)]$$

durch $F(x)$ theilbar sein, und man hat

$$\varphi(x) = F(x)\,f_1(x) + p\chi(x),$$

oder

$$\varphi(x) \equiv F(x)\,f_1(x)\ (mod.\ p),$$

worin $f_1(x)$ eine ganze Function bezeichnet.

Zusatz. — Wenn die nach dem Primzahlmodul p irreductibele ganze Function $F(x)$ in Beziehung auf diesen Modul in keine der Functionen

$$\varphi_1(x)\ ,\ \varphi_2(x)\ ,\ \ldots\ ,\ \varphi_m(x)$$

aufgeht, so geht sie auch nicht in die Function

$$\varphi(x) = \varphi_1(x) \cdot \varphi_2(x) \ldots \varphi_m(x) + p\chi(x)$$

auf, welche nach p dem Produkte der Functionen φ_1, φ_2, ..., φ_m congruent ist.

Dies ergiebt sich unmittelbar aus dem eben bewiesenen Satze.

Bemerkungen über die Zerlegung einer ganzen Function in irreductibele Factoren.

343. Eine ganze Function $\varphi(x)$, welche nach dem Modul p nicht congruent Null ist, kann irreductibel oder reductibel sein. Im letzteren Falle lässt sie sich in irreductibele Factoren zerlegen, und man erhält

$$F(x)\,F_1(x)\,F_2(x) \ldots F_{m-1}(x) = \alpha\varphi(x) + p\chi(x);$$

darin bezeichnen $F(x)$, $F_1(x)$, ... Polynome mit ganzen Coefficienten, die in Beziehung auf den Modul p irreductibel sind,

$\chi(x)$ eine ganze Function und α die Zahl, mit welcher $\varphi(x)$ multiplicirt werden muss, damit der Coefficient der höchsten Potenz von x auf Eins reducirt werde.

Aus dem Zusatz zum vorhergehenden Satze geht hervor, dass die Function $\alpha\varphi(x)$ nur auf eine Art nach dem Modul p in irreductibele Factoren zerlegt werden kann. Dies zu beweisen, nehmen wir an, wir hätten

$$f f_1 f_2 \ldots = F F_1 F_2 \ldots + p\chi(x);$$

$f, \ldots, F, \ldots$ bezeichnen irreductibele Factoren. Der irreductibele Factor F geht in Beziehung auf den Modul p, dem erwähnten Zusatze zufolge, in einen der Factoren des ersten Gliedes, z. B. in f auf, und da auch f irreductibel ist, so müssen die Factoren F und f einander congruent sein. Wir können daher f durch $F + p\chi(x)$ ersetzen; dann geht unsere Formel über in

$$F f_1 f_2 \ldots = F F_1 F_2 \ldots + p\chi(x).$$

Die Function $\chi(x)$ muss durch F theilbar sein, und die Ausführung dieser Division liefert

$$f_1 f_2 \ldots = F_1 F_2 \ldots + p\chi(x).$$

Durch wiederholte Anwendung dieses Schlussverfahrens erhält man das Resultat, dass die Factoren $F, F_1, F_2, \ldots$ beziehungsweise den Factoren $f, f_1, f_2, \ldots$ nach dem Modul p gleich sind.

344. Es kann der Fall eintreten, dass mehrere der irreductibeln Factoren von $\alpha\varphi(x) = \Phi(x)$ einander gleich sind; dann hat die Function $\Phi(x)$ mit ihrer Abgeleiteten einen Divisor gemeinschaftlich. Nehmen wir an, es sei

$$X_1^{n_1} X_2^{n_2} \ldots X_m^{n_m} = \Phi(x) + p\chi(x),$$

wo $X_1, X_2, \ldots, X_m$ Polynome bezeichnen, welche in Beziehung auf den Modul p irreductibel und von einander verschieden sind. Bildet man die Abgeleiteten beider Glieder und stellt allgemein die Abgeleitete von X_i durch X_i' dar, so erhält man

$$X_1^{n_1-1} X_2^{n_2-1} \cdots X_m^{n_m-1} \left(n_1 X_1' X_2 X_3 \cdots X_m + \cdots + n_m X'_m X_1 X_2 \cdots X_{m-1}\right)$$
$$= \Phi'(x) + p\chi'(x).$$

Wenn keiner der Exponenten $n_1, n_2, \ldots, n_m$ ein Vielfaches von p ist, so ist der eingeklammerte Factor durch keinen der irreductibeln Factoren $X_1, X_2, \ldots, X_m$ in Beziehung auf den Modul p theilbar; denn damit derselbe z. B. durch X_1 theilbar sei, müsste X_1 in einen der Factoren des Produkts

$$X_1' X_2 X_3 \ldots X_m$$

aufgehen; dies ist aber unmöglich, da $X_2, X_3, \ldots, X_m$ irreductibel und von X_1 verschieden sind, und da der Grad von X_1' kleiner als derjenige von X_1 ist. Das Produkt der irreductibelen Factoren, welche die Function $\Phi(x)$ mit ihrer Abgeleiteten gemeinschaftlich hat, ist daher

$$X_1^{n_1-1} X_2^{n_2-1} \ldots X_m^{n_m-1}.$$

Dies ist der grösste gemeinschaftliche Divisor dieser Functionen in Beziehung auf den Modul p, und um ihn zu erhalten, hat man die gewöhnliche Regel anzuwenden, bei jeder Division aber die vorkommenden Vielfachen von p zu vernachlässigen und den Coefficienten des höchsten Terms jedes Restes, bevor man diesen als Divisor benutzt, auf die Einheit zu reduciren.

Wenn einer der Exponenten, z. B. n_1, ein Vielfaches von p ist, so geht die n_1^{te} Potenz des Factors X_1 in den grössten gemeinschaftlichen Divisor ein.

Bezeichnet V_1 das Produkt derjenigen der Factoren $X_1, X_2, \ldots$, welche in $\Phi(x)$ mit ein und demselben Exponenten n_1 behaftet sind, V_2 das Produkt derjenigen, welche den Exponenten n_2 haben, u. s. w., so ist

$$V_1^{n_1} V_2^{n_2} V_3^{n_3} \cdots = \Phi(x) + p\chi(x),$$

und durch ein Schlussverfahren, welches mit dem in No. 50 angewandten völlig übereinstimmt, lässt sich beweisen, dass die Factoren $V_1, V_2, V_3, \ldots$ durch einfache algebraische Divisionen ermittelt werden können.

Ganze Functionen einer Veränderlichen, reducirt in Beziehung auf einen Primzahlmodul und in Beziehung auf eine irreductibele ganze Function.

345. Wenn man eine ganze Function $\mathfrak{F}(x)$ durch ein irreductibeles Polynom $F(x)$ von irgend einem Grade ν dividirt, so erhält man einen Quotienten $\varphi(x)$ und einen Rest, welcher durch $f(x) + p\chi(x)$ dargestellt werden kann; $f(x)$ ist eine ganze Function, deren Grad höchstens gleich $\nu - 1$ ist, und deren Coefficienten nach Belieben zwischen den Grenzen 0 und p, oder zwischen $-\frac{p-1}{2}$ und $+\frac{p-1}{2}$ genommen werden können. Man

hat also

$$\mathfrak{F}(x) = f(x) + F(x)\,\varphi(x) + p\chi(x),$$

oder

$$\mathfrak{F}(x) \equiv f(x) + F(x)\,\varphi(x)\ (mod.\ p).$$

Die Function $f(x)$ soll der in Beziehung auf den Modul p und in Beziehung auf die irreductibele Function $F(x)$ reducirte Werth von $\mathfrak{F}(x)$ heissen.

Der allgemeine Ausdruck der reducirten Functionen ist

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{\nu-1}\, x^{\nu-1}.$$

Da jeder der Coefficienten $a_0, a_1, \ldots, a_{\nu-1}$ p verschiedene Werthe, z. B.

$$0, 1, 2, 3, \ldots, (p-1)$$

annehmen kann, so kann die Function $f(x)$ p^ν verschiedene Werthe haben. p dieser Werthe sind von der Veränderlichen x unabhängig; es sind dies die p Zahlen

$$0, 1, 2, 3, \ldots, (p-1).$$

Lehrsatz. — Es seien $X_1, X_2, \ldots, X_m$ m Functionen von x, reducirt in Beziehung auf den Modul p und in Beziehung auf die irreductibele ganze Function $F(x)$. Ferner sei

$$\mathfrak{F}(x) = A_0 X^m + A_1 X^{m-1} + \cdots + A_{m-1} X + A_m$$

eine ganze Function m^{ten} Grades der Veränderlichen X, deren Coefficienten ganze Functionen von x sind. Wir ersetzen X in $\mathfrak{F}(X)$ der Reihe nach durch

$$X_1, X_2, \ldots, X_m;$$

wenn alle dadurch erhaltenen Resultate in Beziehung auf den Modul p durch $F(x)$ theilbar sind, so hat man identisch

$$\mathfrak{F}(X) = A_0 (X - X_1)(X - X_2) \ldots (X - X_m)$$
$$+ F(x)\,\varphi(X, x) + p\chi(X, x),$$

worin φ und χ ganze Functionen der beiden Veränderlichen x und X mit ganzen Coefficienten sind.

Wir betrachten vorläufig $X_1, X_2, \ldots, X_m$ als unbestimmte Grössen und bezeichnen mit $\mathfrak{F}_1(X)$ und R_1 den Quotienten und den Rest der Division von $\mathfrak{F}(X)$ durch $X - X_1$. Ebenso seien $\mathfrak{F}_2(X)$ und R_2 der Quotient und der Rest der Division von $\mathfrak{F}_1(X)$

durch $X-X_2$, u. s. w., endlich $\mathfrak{F}_m(X)$ und R_m der Quotient und der Rest der Division von $\mathfrak{F}_{m-1}(X)$ durch $X-X_m$. Dann liefern die Identitäten

$$(1). \quad \begin{cases} \mathfrak{F}(X) = (X-X_1)\,\mathfrak{F}_1(X) + R_1\,, \\ \mathfrak{F}_1(X) = (X-X_2)\,\mathfrak{F}_2(X) + R_2\,, \\ \cdots\cdots\cdots\cdots \\ \mathfrak{F}_{m-1}(X) = (X-X_m)\,\mathfrak{F}_m(X) + R_m\,, \end{cases}$$

da $\mathfrak{F}_m(X) = A_0$ ist,

$$(2). \quad \begin{cases} \mathfrak{F}(X) = R_1 + R_2(X-X_1) + R_3(X-X_1)(X-X_2) + \cdots \\ \qquad + R_m(X-X_1)\cdots(X-X_{m-1}) \\ \qquad + A_0(X-X_1)\cdots(X-X_m)\,, \end{cases}$$

und man erhält, wenn man X der Reihe nach durch

$$X_1\,,\ X_2\,,\ \ldots\,,\ X_m$$

ersetzt,

$$(3). \quad \begin{cases} \mathfrak{F}(X_1) = R_1\,, \\ \mathfrak{F}(X_2) = R_1 + R_2(X_2-X_1)\,, \\ \mathfrak{F}(X_3) = R_1 + R_2(X_3-X_1) + R_3(X_3-X_1)(X_3-X_2)\,, \\ \cdots\cdots\cdots\cdots \\ \mathfrak{F}(X_m) = R_1 + R_2(X_m-X_1) + \cdots \\ \qquad + R_m(X_m-X_1)\cdots(X_m-X_{m-1}). \end{cases}$$

Wir nehmen jetzt an, $X_1\,, X_2\,, \ldots\,, X_m$ seien ganze Functionen von x, reducirt in Beziehung auf den Modul p und in Beziehung auf die irreductibele Function $F(x)$. Wenn diese Functionen von einander verschieden sind, so kann die Differenz je zweier derselben in Beziehung auf den Modul p nicht durch $F(x)$ theilbar sein, und da dies der Voraussetzung nach mit den ersten Gliedern der Formeln (3) der Fall ist, so müssen die Polynome $R_1\,, R_2\,, \ldots\,, R_m$ in Beziehung auf den Modul p durch $F(x)$ theilbar sein. Dann nimmt die Formel (2) die Form

$$(4). \quad \mathfrak{F}(X) = A_0(X-X_1)\ldots(X-X_m) + F(x)\,\varphi(X,x) + p\chi(X,x)$$

an, und dies war eben zu beweisen.

Zusatz. — Es sei $\mathfrak{F}(X)$ eine ganze Function der beiden Veränderlichen X und x, die in Beziehung auf X vom Grade m ist, und in welcher der Coefficient von X^m in Beziehung auf den Modul p nicht durch die irreductibele Function $F(x)$ theilbar ist. Setzt man an die Stelle von X der Reihe nach die p^ν in Beziehung auf

den Modul p und in Beziehung auf die Function $F(x)$ reducirten Functionen von x, so sind höchstens m der erhaltenen p^ν Resultate durch $F(x)$ nach dem Modul p theilbar.

Nehmen wir an, die m Functionen von x

$$X_1 , X_2 , \ldots , X_m ,$$

reducirt in Beziehung auf den Modul p und in Beziehung auf die Function $F(x)$, seien so beschaffen, dass jede der Functionen

$$\mathfrak{F}(X_1) , \mathfrak{F}(X_2) , \ldots , \mathfrak{F}(X_m)$$

nach dem Modul p durch $F(x)$ theilbar sei. Dann besteht die Formel (4) identisch, und wenn darin X durch eine von

$$X_1 , X_2 , \ldots , X_m$$

verschiedene reducirte Function X_{m+1} ersetzt wird, so hat man

$$\mathfrak{F}(X_{m+1}) = A_0 (X_{m+1} - X_1) \ldots (X_{m+1} - X_m) \\ + F(x)\,\varphi(x) + p\,\chi(x).$$

Nun kann $F(x)$ nach dem Modul p nicht in das Produkt der Differenzen $X_{m+1} - X_1 , X_{m+1} - X_2 , \ldots$ aufgehen; folglich ist $\mathfrak{F}(X_{m+1})$ nach diesem Modul durch das Polynom $F(x)$ nicht theilbar.

Fundamental-Eigenschaften der nach einem Primzahlmodul irreductibelen Polynome.

346. Lehrsatz I. — Jedes Polynom $F(x)$ mit ganzen Coefficienten und vom Grade ν, welches in Beziehung auf den Primzahlmodul p irreductibel ist, geht nach diesem Modul in die Function $x^{p^\nu} - x$ auf.

Der allgemeine Ausdruck der in Beziehung auf den Modul p und in Beziehung auf die irreductibele Function $F(x)$ reducirten ganzen Functionen von x ist

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{\nu-1} x^{\nu-1};$$

$a_0 , a_1 , \ldots , a_{\nu-1}$ sind ganze Zahlen, die zwischen 0 und p, oder zwischen $-\frac{p-1}{2}$ und $+\frac{p-1}{2}$ liegen. Eine dieser Functionen ist Null; wir abstrahiren von derselben und bezeichnen die $p^\nu - 1$ von Null verschiedenen reducirten Functionen mit

(1). $$X_1 , X_2 , \ldots , X_{p^\nu - 1} .$$

Dies vorausgesetzt, sei $f(x)$ eine nach dem Modul p durch $F(x)$ nicht theilbare ganze Function von x; wir betrachten die Produkte der Functionen (1) in $f(x)$, nämlich

(2). $$X_1 f(x)\ ,\ X_2 f(x)\ ,\ \ldots,\ X_{p^\nu-1} f(x).$$

Keines dieser Produkte ist nach dem Modul p durch das irreductibele Polynom $F(x)$ theilbar, da die Factoren, aus denen es besteht, diesen Divisor nicht zulassen. Offenbar kann aber auch die Differenz zweier Terme der Reihe (2) nicht durch $F(x)$ nach dem Modul p theilbar sein, da diese Differenz selbst ein Term von (2) ist. Die in Beziehung auf den Modul p und in Beziehung auf das irreductibele Polynom $F(x)$ reducirten Werthe der Produkte (2) sind daher von einander verschieden, und keiner von ihnen ist Null: folglich fallen sie, abgesehen von der Reihenfolge, mit den Termen der Reihe (1) zusammen. Daraus geht hervor, dass zwischen den Functionen der Reihe (2) und den entsprechenden Functionen von (1) $p^\nu - 1$ Congruenzen von der Form

$$X_m f(x) \equiv X_n + F(x)\ \varphi(x)\ (mod.\ p)$$

bestehen, durch deren Multiplication sich

$$X_1 X_2 \ldots X_{p^\nu-1} \left[f(x)^{p^\nu-1} - 1\right] \equiv F(x)\ \varphi(x)\ (mod.\ p)$$

ergiebt, worin φ eine ganze Function von x darstellt. Das Produkt $X_1\ X_2\ \ldots\ X_{p^\nu-1}$ ist in Beziehung auf den Modul p durch $F(x)$ nicht theilbar, mithin hat man

(3). $$f(x)^{p^\nu-1} - 1 \equiv F(x)\ \varphi(x)\ (mod.\ p),$$

oder, wenn man mit $f(x)$ multiplicirt,

(4). $$f(x)^{p^\nu} - f(x) \equiv F(x)\ \varphi(x)\ (mod.\ p).$$

Wir haben vorausgesetzt, die Function $f(x)$ sei nach dem Modul p nicht durch $F(x)$ theilbar; es liegt aber auf der Hand, dass die Formel (4) auch dann gültig bleibt, wenn $f(x)$ ein Vielfaches von $F(x)$ ist.

Da die Formel (4) für jeden Werth der ganzen Function $f(x)$ besteht, so können wir $f(x) = x$ annehmen; dann ist

(5). $$x^{p^\nu} - x \equiv F(x)\ \varphi(x)\ (mod.\ p),$$

also unser Satz bewiesen.

347. Hilfssatz. — Es seien $f(x)$ eine ganze Function der Veränderlichen x, p eine Primzahl und n irgend eine ganze Zahl; dann hat man

$$f(x^{p^n}) = [f(x)]^{p^n} + p\chi(x),$$

worin $\chi(x)$ eine ganze Function bezeichnet.

Es sei

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m.$$

Die p^{te} Potenz von $f(x)$ besteht erstens aus den p^{ten} Potenzen der verschiedenen Terme, ferner aus Termen, welche gewisse Potenzen mehrerer Terme von $f(x)$ enthalten; der Coefficient irgend eines dieser letzteren Terme hat die Form

$$\frac{1 \cdot 2 \cdots p}{(1 \cdot 2 \cdots q_1) \cdots (1 \cdot 2 \cdots q_k)}.$$

Da nun jede der Zahlen $q_1, q_2, \ldots, q_k$ kleiner als p ist, so ist dieser Coefficient durch p theilbar, und man hat

$$[f(x)]^p + p\chi(x) = a_0^p + a_1^p x^p + a_2^p x^{2p} + \cdots + a_m^p x^{mp}.$$

Nach dem Fermat'schen Satze ist aber

$$a^p \equiv a \pmod{p},$$

folglich

$$[f(x)]^p + p\chi(x) = a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_m x^{mp},$$

oder

$$f(x^p) = [f(x)]^p + p\chi(x);$$

darin bezeichnet $\chi(x)$ eine ganze Function.

Schreibt man $x^{p^{n-1}}$ statt x, so folgt

$$f(x^{p^n}) = [f(x^{p^{n-1}})]^p + p\chi(x),$$

und hier bezeichnet $\chi(x)$ eine neue ganze Function.

Dies vorausgesetzt, nehmen wir an, es sei

$$f(x^{p^{n-1}}) = [f(x)]^{p^{n-1}} + p\chi(x);$$

wird diese Formel auf die p^{te} Potenz erhoben, so ergiebt sich mit Rücksicht auf die vorhergehende Relation

$$f(x^{p^n}) = [f(x)]^{p^n} + p\chi(x).$$

Wenn demnach diese Formel für einen Werth des Exponenten n besteht, so besteht sie auch für den nächst höheren Werth; da sie nun für $n = 1$ bewiesen ist, so muss sie allgemein gültig sein.

348. Lehrsatz II. — Eine ganze Function ν^{ten} Grades $F(x)$, welche in Beziehung auf den Primzahlmodul

p irreductibel ist, geht nur dann nach diesem Modul in $x^{p^\mu} - x$ auf, wenn μ ein Vielfaches von ν ist.

Wir zeigen zunächst, dass die Function $x^{p^\mu} - x$, wenn $\mu < \nu$ ist, nach dem Modul p durch $F(x)$ nicht theilbar sein, d. h. dass man nicht haben kann:

$$(1). \qquad x^{p^\mu} - x = F(x)\,\varphi(x) + p\chi(x),$$

worin $\varphi(x)$ und $\chi(x)$ Polynome mit ganzen Coefficienten sind. Dies zu beweisen, nehmen wir an, die Relation (1) bestehe, und setzen

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{\nu-1} x^{\nu-1};$$

$a_0, a_1, \ldots$ sind irgend welche zwischen 0 und $p-1$ enthaltene ganze Zahlen. Nach dem vorhergehenden Hilfssatze ist

$$[f(x)]^{p^\mu} = f(x^{p^\mu}) + p\chi_1(x),$$

worin $\chi_1(x)$ eine ganze Function bezeichnet, und wenn im zweiten Gliede dieser Identität x^{p^μ} durch den aus (1) genommenen Werth $x + F(x)\,\varphi(x) + p\chi(x)$ ersetzt wird, so nimmt dieses Glied offenbar die Form

$$f(x) + F(x)\,\Phi(x) + p\Psi(x)$$

an, wo Φ und Ψ Polynome mit ganzen Coefficienten darstellen; es ist daher

$$(2). \qquad [f(x)]^{p^\mu} - f(x) = F(x)\,\Phi(x) + p\Psi(x).$$

Aus dieser Formel (2) geht hervor, dass, wenn man in der Function $(p^\mu)^{\text{ten}}$ Grades

$$X^{p^\mu} - X$$

X durch jede der in Beziehung auf den Modul p und die Function $F(x)$ reducirten p^ν Functionen ersetzt, man p^ν Resultate erhält, welche sämmtlich nach dem Modul p durch $F(x)$ theilbar sind. Dies ist aber nach No. 345 für $\mu < \nu$ unmöglich; mithin kann die Formel (1) in diesem Falle nicht stattfinden.

Zweitens behaupten wir, dass die Formel (1) nur dann bestehen kann, wenn μ durch ν theilbar ist. Es sei nämlich q der Quotient und r der Rest der Division von μ durch ν, also

$$\mu = \nu q + r.$$

Nach dem Lehrsatz I (No. 346) geht $F(x)$ in Beziehung auf den Modul p in die Function

$$x^{p^\nu} - x = x\,[x^{p^\nu - 1} - 1]$$

auf, und diese geht algebraisch in

$$x\left(x^{p^{\nu q}-1} - 1\right) = x^{p^{\nu q}} - x$$

auf, da der Exponent $p^{\nu q} - 1$ ein Vielfaches von $p^\nu - 1$ ist. Folglich ist $x^{p^{\nu q}} - x$ nach dem Modul p durch $F(x)$ theilbar. Der Voraussetzung nach geht $F(x)$ nach dem Modul p aber auch in die Function $x^{p^\mu} - x$ auf; daher muss auch die Differenz

$$(x^{p^\mu} - x) - (x^{p^{\nu q}} - x) = x^{p^{\nu q + r}} - x^{p^{\nu q}}$$

nach dem Modul p durch $F(x)$ theilbar sein. Dem Hilfssatze der No. 347 zufolge ist diese Differenz nach dem Modul p der Potenz

$$\left(x^{p^r} - x\right)^{p^{\nu q}}$$

congruent, und diese Potenz kann nur dann nach dem Modul p durch $F(x)$ theilbar sein, wenn

$$x^{p^r} - x$$

in Beziehung auf denselben Modul durch $F(x)$ theilbar ist. Da aber $r < \nu$ ist, so ist dies, wie wir oben gesehen haben, nur für $r = 0$ möglich.

Bestimmung der Anzahl der ganzen Functionen ν^{ten} Grades, welche in Beziehung auf einen Primzahlmodul p irreductibel sind.

349. Wir sind jetzt im Stande zu beweisen, dass es ganze Functionen jeden Grades ν giebt, welche in Beziehung auf einen Primzahlmodul p irreductibel sind; auch ist es leicht, wie man sehen wird, die Anzahl dieser Functionen zu bestimmen.

Wir betrachten die Function $x^{p^\nu} - x$ und setzen voraus, dieselbe sei in Factoren, die nach dem Modul p irreductibel sind, zerlegt, d. h. es sei

$$F(x)\ F_1(x)\ F_2(x) \ldots = x^{p^\nu} - x + p\chi(x),$$

worin $F(x)$, $F_1(x)$, $F_2(x)$, u. s. w. ganze, nach dem Modul p irreductibele Functionen sind und $\chi(x)$ irgend eine ganze Function bezeichnet.

Es ist unmöglich, dass zwei der Factoren F, F_1, F_2, u. s. w.

einander gleich sind, da die Function $x^{p^\nu} - x$ keinen Factor mit ihrer Abgeleiteten gemeinschaftlich hat. Ausserdem führen die früheren Entwicklungen zu folgenden Ergebnissen:

1^0. Jede nach dem Modul p irreductibele ganze Function ν^{ten} Grades ist in der Reihe $F(x)$, $F_1(x)$, $F_2(x)$, u. s. w. enthalten.

2^0. Der Grad irgend einer Function dieser Reihe ist gleich ν oder gleich einem Divisor von ν.

3^0. Diejenigen der Functionen $F(x)$, $F_1(x)$, $F_2(x)$, u. s. w., deren Grad ein Divisor μ von ν ist ($\mu < \nu$), gehen nach dem Modul p in die Function $x^{p^\mu} - x$ auf.

Daraus geht hervor, dass, wenn man die Function $x^{p^\nu} - x$ nach dem Modul p durch das Produkt aller irreductibelen Functionen dividirt, welche in eine der Functionen $x^{p^\mu} - x$, wo μ ein Divisor von ν ist, aufgehen, man einen Quotienten V erhält, welcher das Produkt aller nach dem Modul p irreductibelen ganzen Functionen ν^{ten} Grades ist.

Wenn z. B. ν eine Primzahl ist, so sind die irreductibelen Factoren von $x^{p^\nu} - x$ sämmtlich vom Grade ν oder vom Grade 1; das Produkt der Factoren ersten Grades ist

$$x(x-1)(x-2)\ldots(x-p+1), \text{ oder } x^p - x.$$

Man hat daher in diesem Falle

$$V = \frac{x^{p^\nu} - x}{x^p - x}.$$

Der Grad von V ist hier $p^\nu - p$; folglich ist die Anzahl N der in Beziehung auf einen Primzahlmodul p irreductibelen ganzen Functionen, deren Grad ν eine Primzahl ist, gleich

$$N = \frac{p^\nu - p}{\nu}.$$

Wir wenden uns jetzt zum allgemeinen Falle: es sei

$$\nu = q_1^{n_1} q_2^{n_2} \ldots q_m^{n_m},$$

worin $q_1, q_2, \ldots, q_m$ ungleiche Primzahlen und $n_1, n_2, \ldots, n_m$ irgend welche ganze positive Zahlen sind. Der Kürze wegen setzen wir für jeden Werth der ganzen Zahl λ

$$x^{p^\lambda} - x = [\lambda],$$

und machen ausserdem

$$X = \left[\nu \right],$$

$$X_1 = \left[\frac{\nu}{q_1} \right] \left[\frac{\nu}{q_2} \right] \cdots \left[\frac{\nu}{q_m} \right],$$

$$X_2 = \left[\frac{\nu}{q_1 q_2} \right] \left[\frac{\nu}{q_1 q_3} \right] \cdots \left[\frac{\nu}{q_{m-1} q_m} \right],$$

$$\cdots\cdots\cdots\cdots,$$

$$X_m = \left[\frac{\nu}{q_1 q_2 \cdots q_m} \right];$$

danach ist X_k das Produkt von

$$\frac{m(m-1)\ldots(m-k+1)}{1.2\ldots k}$$

Symbolen [ ], und die Nenner der Argumente dieser Symbole sind die Produkte von je k der m Zahlen $q_1, q_2, \ldots, q_m$. Dies vorausgesetzt, behaupten wir, es sei

$$V = \frac{X X_2 X_4 X_6 \ldots}{X_1 X_3 X_5 \ldots}.$$

Wir denken uns, der Zähler und der Nenner dieses Ausdrucks seien in irreductibele Factoren zerlegt, und bezeichnen einen dieser Factoren mit $F(x)$. Wenn der Factor $F(x)$ vom Grade ν ist, so tritt er nur in X auf; folglich hat er im Zähler des vorstehenden Ausdrucks den Exponenten 1, im Nenner den Exponenten Null.

Wenn der Grad μ von $F(x)$ kleiner als ν ist, so gehen einige der Primfactoren q in ν wenigstens einmal mehr als in μ ein; werden diese Factoren, deren Anzahl s sich auch auf 1 reduciren kann, mit $q_1, q_2, \ldots, q_s$ bezeichnet, so geht der Grad μ in

$$\frac{\nu}{q_1 q_2 \cdots q_s},$$

aber nicht in den Quotienten von ν durch einen neuen Factor q, wie q_{s+1}, auf. Der irreductibele Factor $F(x)$ tritt in X in der ersten Potenz auf; wir wollen allgemein bestimmen, mit welchem Exponenten er sich in X_k vorfindet. Hat man $k > s$, so ist der Factor $F(x)$ in der Function X_k nicht enthalten; wenn aber $k < s$ oder $k = s$ ist, so enthält X_k offenbar so viele Factoren, die gleich $F(x)$ sind, als es Combinationen von s Elementen zur k^{ten} Klasse giebt. Da die Anzahl dieser Combinationen gleich

$$\frac{s(s-1)\ldots(s-k+1)}{1\cdot 2\cdots k}$$

ist, so enthalten der Zähler und der Nenner des vorhergehenden Ausdrucks den Factor $F(x)$ mit Exponenten, welche beziehungsweise den folgenden Summen gleich sind:

$$1 + \frac{s(s-1)}{1\cdot 2} + \frac{s(s-1)(s-2)(s-3)}{1\cdot 2\cdot 3\cdot 4} + \cdots$$

und

$$\frac{s}{1} + \frac{s(s-1)(s-2)}{1\cdot 2\cdot 3} + \frac{s(s-1)\cdots(s-4)}{1\cdot 2\cdot 3\cdot 4\cdot 5} + \cdots.$$

Diese beiden Summen sind aber einander gleich; denn ihre Differenz ist offenbar gleich $(1-1)^s$ oder gleich Null. Folglich ist der Zähler unseres Ausdrucks in Beziehung auf den Modul p durch den Nenner theilbar, und der Quotient der Division ist gleich dem Producte V aller ganzen Functionen ν^{ten} Grades, welche nach dem Modul p irreductibel sind.

Es ist übrigens gut, zu beachten, dass der Zähler des Ausdrucks von V algebraisch durch den Nenner theilbar ist. Dies zu beweisen, genügt es, das eben angewandte Schlussverfahren zu wiederholen, und dabei durch μ immer einen Divisor von ν darzustellen, zugleich auch das Polynom μ^{ten} Grades $F(x)$ durch einen der linearen Factoren zu ersetzen, welche algebraisch in $x^{p^\mu} - x$, aber nicht in $x^{p^{\mu_1}} - x$ $(\mu_1 < \mu)$ aufgehen. Der Grad des Polynoms V kann durch

$$p^\nu - \sum p^{\frac{\nu}{q_1}} + \sum p^{\frac{\nu}{q_1 q_2}} - \cdots + (-1)^{m-1} \sum p^{\frac{\nu}{q_1 q_2 \cdots q_{m-1}}} + (-1)^m p^{\frac{\nu}{q_1 q_2 \cdots q_m}}$$

dargestellt werden, und da dieses Polynom das Produkt aller N ganzen Functionen ν^{ten} Grades ist, welche in Beziehung auf den Modul p irreductibel sind, so hat man

$$N = \frac{p^\nu - \sum p^{\frac{\nu}{q_1}} + \cdots + (-1)^{m-1} \sum p^{\frac{\nu}{q_1 q_2 \cdots q_{m-1}}} + (-1)^m p^{\frac{\nu}{q_1 q_2 \cdots q_m}}}{\nu}.$$

350. Aus der vorstehenden Formel kann man zwei sehr einfache Grenzen für die Anzahl N der nach dem Primzahlmodul p irreductibeln Congruenzen ν^{ten} Grades entnehmen. Geht man nämlich von der Formel

$$p^t = 1 + \frac{t \log p}{1} + \frac{t^2 \log^2 p}{1 \cdot 2} + \cdots$$

aus, so hat man

$$\begin{aligned}N = & \left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \cdots \left(1 - \frac{1}{q_m}\right) \frac{\log p}{1} \\ & + \left(1 - \frac{1}{q_1^2}\right)\left(1 - \frac{1}{q_2^2}\right) \cdots \left(1 - \frac{1}{q_m^2}\right) \frac{\nu \log^2 p}{1 \cdot 2} \\ & + \cdots\cdots\cdots \\ & + \left(1 - \frac{1}{q_1^k}\right)\left(1 - \frac{1}{q_2^k}\right) \cdots \left(1 - \frac{1}{q_m^k}\right) \frac{\nu^{k-1} \log^k p}{1 \cdot 2 \cdots k} \\ & + \cdots\cdots\cdots ;\end{aligned}$$

darin sind überall natürliche Logarithmen gemeint.

Aus dieser Formel folgt zunächst

$$N < \left(1 - \frac{1}{\nu}\right) \frac{\log p}{1} + \left(1 - \frac{1}{\nu^2}\right) \frac{\nu \log^2 p}{1 \cdot 2} + \left(1 - \frac{1}{\nu^3}\right) \frac{\nu^2 \log^3 p}{1 \cdot 2 \cdot 3} + \cdots,$$

oder

$$N < \frac{p^\nu - p}{\nu},$$

ferner

$$N > \frac{\varphi(\nu)}{\nu} \left(\frac{\log p}{1} + \frac{1 - \frac{1}{\nu^2}}{1 - \frac{1}{\nu}} \frac{\nu \log^2 p}{1 \cdot 2} + \frac{1 - \frac{1}{\nu^3}}{1 - \frac{1}{\nu}} \frac{\nu^2 \log^3 p}{1 \cdot 2 \cdot 3} + \cdots \right),$$

oder

$$N > \frac{\varphi(\nu)}{\nu - 1} \frac{p^\nu - p}{\nu},$$

wo $\varphi(\nu)$ die Gesammtzahl der Zahlen bezeichnet, die prim zu ν und kleiner als ν sind. Jede der ermittelten Grenzen drückt den Werth von N aus, wenn ν eine Primzahl ist.

Ueber die Zerlegung einer gegebenen ganzen Function in Factoren, die nach einem Primzahlmodul irreductibel sind.

351. Wenn es sich darum handelt, eine gegebene Function $\mathfrak{F}(x)$ in Factoren zu zerlegen, welche nach dem Modul p irreductibel sind, so hat man zunächst zu untersuchen, ob diese Function vielfache Divisoren besitzt. Wenn dies der Fall ist, so ist sie von der Form

$$\mathfrak{F}(x) \equiv V_1^{n_1} V_2^{n_2} V_3^{n_3} \dots (mod.\ p),$$

wo V_1, V_2, ... ganze Functionen sind, welche nur einfache Factoren zulassen, und die nach No. 344 durch einfache algebraische Divisionen bestimmt werden können.

Die Aufgabe ist somit auf den Fall zurückgeführt, in welchem $\mathfrak{F}(x)$ nur einfache Factoren enthält; dann hat die Function $\mathfrak{F}(x)$ mit ihrer Abgeleiteten keinen Factor nach dem Modul p gemeinschaftlich.

Dies vorausgesetzt, erhält man das Produkt der irreductibelen Factoren ersten Grades von $\mathfrak{F}(x)$, wenn man den grössten gemeinschaftlichen Divisor der Polynome $\mathfrak{F}(x)$ und $x^p - x$ ermittelt. Wir bezeichnen diesen Divisor, der sich auch auf Eins reduciren kann, mit P_1 und setzen

$$\mathfrak{F}(x) \equiv P_1 \mathfrak{F}_1(x) \ (mod.\ p),$$

wo $\mathfrak{F}_1(x)$ eine ganze Function ist.

Weiter erhält man das Produkt der irreductibelen Factoren zweiten Grades von $\mathfrak{F}(x)$ oder von $\mathfrak{F}_1(x)$, wenn man den grössten gemeinschaftlichen Divisor der Polynome $\mathfrak{F}_1(x)$ und $x^{p^2} - x$ bestimmt, und wenn dieser Divisor, der sich gleichfalls auf Eins reduciren kann, mit P_2 bezeichnet wird, so hat man

$$\mathfrak{F}_1(x) \equiv P_2 \mathfrak{F}_2(x) \ (mod.\ p),$$

wo $\mathfrak{F}_2(x)$ eine ganze Function ist.

Ebenso liefert der grösste gemeinschaftliche Divisor P_3 der Functionen $\mathfrak{F}_2(x)$ und $x^{p^3} - x$, wenn er sich nicht auf Eins reducirt, das Produkt der Divisoren dritten Grades; es ist

$$\mathfrak{F}_2(x) \equiv P_3 \mathfrak{F}_3(x) \ (mod.\ p),$$

u. s. w. So fortfahrend, muss man offenbar zu einer Function $\mathfrak{F}_m(x)$ gelangen, welche sich auf Eins reducirt, und es ist

$$\mathfrak{F}(x) \equiv P_1 P_2 P_3 \dots P_m \ (mod.\ p).$$

Um die Lösung der Aufgabe zu vollenden, hat man noch jedes der Polynome P_ν in irreductibele Factoren ν^{ten} Grades zu zerlegen. Die allgemeinste Methode, welche dies leistet, besteht im Folgenden: Man dividirt das Polynom P_ν durch die Function

$$F(x) = x^\nu + A_1 x^{\nu-1} + A_2 x^{\nu-2} + \cdots + A_{\nu-1} x + A_\nu,$$

deren Coefficienten unbestimmt sind, und drückt sodann aus, dass die ν Terme des Restes nach dem Modul p congruent Null seien. Dadurch erhält man ein System von ν Congruenzen, mittels wel-

cher die ν Coefficienten $A_1, A_2, \ldots, A_\nu$ bestimmt werden können. Bezeichnet $\mu\nu$ den Grad von P_ν, so wird dies Congruenzensystem augenscheinlich μ Lösungssysteme zulassen, welche beziehungsweise den μ irreductibelen Polynomen ν^{ten} Grades entsprechen, deren Produkt gleich P_ν ist.

Die Aufgabe, alle ganzen Functionen ν^{ten} Grades zu suchen, welche nach dem Modul p irreductibel sind, ist ein specieller Fall der im Vorhergehenden behandelten Aufgabe. Letztere geht nämlich in jene über, wenn in der vorstehenden Entwicklung

$$\mathfrak{F}(x) = x^{p^\nu} - x$$

gesetzt wird.

Classification der nach dem Primzahlmodul p irreductibelen ganzen Functionen ν^{ten} Grades.

352. Wenn n ein Divisor von $p^\nu - 1$ ist, so geht die Function $x^n - 1$ in $x^{p^\nu-1} - 1$ oder in $x^{p^\nu} - x$ auf. Wird daher $x^n - 1$ in Factoren zerlegt, die nach dem Modul p irreductibel sind, so dass man

$$F(x)\ F_1(x)\ F_2(x) \ldots = x^n - 1 + p\chi(x)$$

hat, wo $\chi(x)$ eine ganze Function ist, so sind die Functionen $F(x)$, $F_1(x)$, ... unter den irreductibelen Factoren von $x^{p^\nu} - x$ enthalten, und ihr Grad ist folglich gleich ν oder gleich einem Divisor von ν.

Wenn $F(x)$ eine nach dem Modul p irreductibele ganze Function ν^{ten} Grades ist, und wenn n die kleinste Zahl von der Beschaffenheit darstellt, dass $x^n - 1$ durch $F(x)$ nach dem Modul p theilbar ist, so sagen wir: Die Function $F(x)$ gehört zum Exponenten n. Es liegt auf der Hand, dass n ein Divisor von $p^\nu - 1$ ist; denn da $F(x)$ nach dem Modul p in die beiden Functionen $x^{p^\nu-1} - 1$ und $x^n - 1$ aufgeht, so ist $F(x)$ auch ein Divisor von $x^\vartheta - 1$, wenn ϑ den grössten gemeinschaftlichen Divisor der beiden Zahlen $p^\nu - 1$ und n bezeichnet, und da $F(x)$ zum Exponenten n gehört, so muss $\vartheta = n$ sein. Man sieht auch, dass n ein $p^\nu - 1$ eigener Divisor sein muss, d. h. dass n nicht in $p^\mu - 1$ aufgehen kann, wenn $\mu < \nu$ ist. Fände nämlich das Gegentheil statt, so würde $x^n - 1$ ein Divisor von $x^{p^\mu-1} - 1$, diese letztere Function also nach dem Modul p durch

$F(x)$ theilbar sein, was unter der Voraussetzung $\mu < \nu$ unmöglich ist.

Dies vorausgesetzt, stellen wir uns die Aufgabe, die Anzahl der ganzen Functionen ν^{ten} Grades zu bestimmen, welche nach dem Primzahlmodul p irreductibel sind, und die zu einem Exponenten n gehören, welcher ein $p^\nu - 1$ eigener Divisor ist.

Es sei

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_m^{\alpha_m},$$

wo $q_1, q_2, \dots, q_m$ ungleiche Primzahlen sind. Wir setzen ferner

$$X = x^n - 1,$$

$$X_1 = \left(x^{\frac{n}{q_1}} - 1\right)\left(x^{\frac{n}{q_2}} - 1\right) \dots \left(x^{\frac{n}{q_m}} - 1\right),$$

$$X_2 = \left(x^{\frac{n}{q_1 q_2}} - 1\right)\left(x^{\frac{n}{q_1 q_3}} - 1\right) \dots \left(x^{\frac{n}{q_{m-1} q_m}} - 1\right),$$

$$\dots\dots\dots\dots,$$

$$X_m = \left(x^{\frac{n}{q_1 q_2 \dots q_m}} - 1\right);$$

danach ist X_k das Produkt von

$$\frac{m(m-1)\dots(m-k+1)}{1.2\dots k}$$

Factoren, welche aus

$$x^{\frac{n}{\vartheta_k}} - 1$$

dadurch hervorgehen, dass man für ϑ_k die Produkte von je k der Factoren $q_1, q_2, \dots, q_m$ nimmt. Bezeichnet endlich V das Produkt aller ganzen Funktionen ν^{ten} Grades, welche nach dem Modul p irreductibel sind und zum Exponenten n gehören, so behaupten wir, es sei

$$V = \frac{X X_2 X_4 X_6 \dots}{X_1 X_3 X_5 \dots}.$$

Wir beweisen diese Behauptung mittels eines Schlussverfahrens, welches dem in No. 349 angewandten ganz ähnlich ist. Denken wir uns die beiden Terme des Ausdrucks von V in irreductibele Factoren zerlegt; einer dieser Factoren sei $F(x)$. Wenn die Function $F(x)$ zum Exponenten n gehört, so tritt sie nur in X auf, und hat folglich im Zähler von V den Exponenten 1, im Nenner den Exponenten Null. Gehört aber $F(x)$ zum Exponenten $m < n$, so geht m in die Quotienten auf, welche sich erge-

ben, wenn man n durch einige der Faktoren q, z. B. durch $q_1, q_2, \ldots, q_s$ dividirt. Der Factor $F(x)$ tritt dann in X in der ersten Potenz auf; er kommt in X_k gar nicht vor, wenn $k > s$ ist; hat man aber $k < s$, so besitzt $F(x)$ in X_k den Exponenten

$$\frac{s(s-1)\cdots(s-k+1)}{1\,.\,2\ldots k},$$

welcher gleich der Anzahl der Combinationen von s Elementen zur k^{ten} Klasse ist. Daraus ergiebt sich, dass der Factor $F(x)$ in dem Ausdruck von V den Exponenten

$$1 - \frac{s}{1} + \frac{s(s-1)}{1\,.\,2} - \cdots = (1-1)^s = 0$$

hat, und folglich ist V gleich dem Produkte aller irreductibeln Functionen ν^{ten} Grades, welche zum Exponenten n gehören; die Anzahl dieser Functionen bezeichnen wir mit N.

Der Grad der Function V ist

$$n - \left(\frac{n}{q_1} + \frac{n}{q_2} + \cdots + \frac{n}{q_m}\right) + \left(\frac{n}{q_1 q_2} + \frac{n}{q_1 q_3} + \cdots\right) - \cdots$$

$$\pm \frac{n}{q_1 q_2 \cdots q_m},$$

oder

$$n\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\cdots\left(1 - \frac{1}{q_m}\right).$$

Man hat daher

$$N = \frac{1}{\nu}\cdot n\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\cdots\left(1 - \frac{1}{q_m}\right),$$

oder

$$N = \frac{\varphi(n)}{\nu},$$

wenn $\varphi(n)$ die Anzahl der ganzen Zahlen bezeichnet, die prim zu n und kleiner als n sind.

Wenn n ein Primzahl ist, so reducirt sich die vorstehende Formel auf

$$N = \frac{n-1}{\nu},$$

und daraus folgt

$$n = \nu N + 1.$$

Danach hat jede Primzahl, die ein $p^\nu - 1$ eigener Divisor ist, die Form $k\nu + 1$, was mit einem Satze von Euler übereinstimmt.

353. Aus dem Vorhergehenden ist ersichtlich, dass die in Beziehung auf den Modul p irreductibelen ganzen Functionen ν^{ten} Grades sich nach dem Exponenten, zu welchem sie gehören, naturgemäss in mehrere Klassen vertheilen. Eine dieser Klassen umfasst die Functionen, welche zum Exponenten $p^\nu - 1$ gehören, und welche in der Theorie, die uns jetzt beschäftigt, eine wichtige Rolle spielen. Sie haben z. B. die in dem folgenden Satze enthaltene bemerkenswerthe Eigenschaft.

Lehrsatz. — Wenn $F(x)$ eine nach dem Modul p irreductibele ganze Function ν^{ten} Grades bezeichnet, die zum Exponenten $p^\nu - 1$ gehört, so erhält man die nach dem Modul p verschiedenen $p^\nu - 1$ ganzen Functionen $(\nu - 1)^{\text{ten}}$ Grades dadurch, dass man die Reste nimmt, welche sich bei den Divisionen der Potenzen

$$x\ ,\ x^2\ ,\ x^3\ ,\ \ldots\ ,\ x^{p^\nu - 1}$$

durch $F(x)$ ergeben.

Zwei dieser Potenzen, x^m und x^{n+m}, können nämlich, wenn man sie durch $F(x)$ dividirt, nicht Reste $(\nu - 1)^{\text{ten}}$ Grades liefern, die nach dem Modul p congruent sind; denn sonst würde der Ausdruck

$$x^{n+m} - x^m \text{ oder } x^m(x^n - 1),$$

und mithin auch $x^n - 1$ nach dem Modul p durch $F(x)$ theilbar sein, und dies ist unmöglich, da n kleiner ist, als der Exponent $p^\nu - 1$, zu welchem $F(x)$ gehört.

354. Aus der dargelegten Theorie ergiebt sich weiter der folgende wichtige Satz:

Lehrsatz. — Wenn n eine Primzahl, a eine primitive Wurzel von n und der Modul p von der Form $a + kn$ ist, so ist die Function

$$V = \frac{x^n - 1}{x - 1}$$

in Beziehung auf den Modul p irreductibel.

n ist nämlich eine Primzahl; ausserdem ist n ein $p^{n-1} - 1$ eigener Divisor, da $p - kn$ eine primitive Wurzel von n ist; folglich ist die Anzahl der nach dem Modul p irreductibeln Factoren von V hier gleich $\frac{\varphi(n)}{n-1}$ oder gleich 1.

Zusatz. — Wenn n eine Primzahl ist, so ist die Function $\frac{x^n - 1}{x - 1}$ **algebraisch** irreductibel.

Es sei nämlich a eine primitive Wurzel von n. Lejeune-Dirichlet hat nachgewiesen, dass die arithmetische Progression

$$a\,,\, a+n\,,\, a+2n\,,\, a+3n\,,\,\ldots$$

unendlich viele Primzahlen enthält. Eine dieser Primzahlen sei

$$p = a + kn;$$

dann ist die Function $\frac{x^n - 1}{x - 1}$ nach dem Modul p, folglich um so mehr algebraisch irreductibel.

Vergleichnng der nach dem Modul p irreductibelen ganzen Functionen, welche zu Exponenten gehören, die aus denselben Primfactoren gebildet sind.

355. Wenn n durch den Modul p theilbar, wenn etwa $n = pn'$ ist, so erhält man

$$x^n - 1 \equiv (x^{n'} - 1)^p \ (mod.\ p),$$

und mithin ist die Function $x^n - 1$ auf $x^{n'} - 1$ zurückgeführt.

Wir setzen voraus, n sei nicht durch p theilbar. Bezeichnet dann ν die kleinste Zahl von der Beschaffenheit, dass $p^\nu - 1$ durch n theilbar ist, so geht die Function $x^n - 1$ nach dem Modul p in $x^{p^\nu} - x$ auf, und der Grad jedes ihrer irreductibelen Factoren ist, wie wir gesehen haben, gleich ν oder gleich einem Divisor von ν. Diejenigen dieser Factoren, die zum Exponenten n gehören, sind aber sämmtlich vom Grade ν, und wir haben oben gefunden, dass ihre Anzahl gleich $\frac{\varphi(n)}{\nu}$ ist, wo φ die gewöhnliche Bedeutung hat.

Bezeichnen wir, dies vorausgesetzt, mit μ die kleinste Zahl, die so beschaffen ist, dass jeder Primfactor von n in $p^\mu - 1$ aufgeht, so ist ν offenbar ein Vielfaches von μ. Es sei nämlich

$$\nu = \mu q + r;$$

die Primfactoren von n gehen der Voraussetzung nach in

$$p^{\mu q + r} - 1$$

und ebenso in die Grösse $p^{\mu q} - 1$ auf, welche ein Vielfaches von $p^\mu - 1$ ist; sie müssen daher auch in die Differenz

$$p^{\mu q+r} - p^{\mu q} \text{ oder } p^{\mu q}(p^r - 1)$$

aufgehen. Dies ist aber, da $r < \mu$ ist, nur für $r = 0$ möglich; man hat daher

(1).
$$\nu = q\mu.$$

Es sei $\frac{p^\mu - 1}{d}$ der grösste gemeinschaftliche Divisor der Zahlen n und $p^\mu - 1$. Macht man

(2).
$$n = \frac{p^\mu - 1}{d}\,\lambda,$$

so sind λ und d relative Primzahlen; es folgt sodann

(3).
$$\frac{p^\nu - 1}{n} = \frac{d}{\lambda} \cdot \frac{p^{\mu q} - 1}{p^\mu - 1},$$

und da das erste Glied dieser Formel eine ganze Zahl ist, so muss λ ein Divisor von $\frac{p^{\mu q} - 1}{p^\mu - 1}$ sein. Erhebt man die Identität

$$p^\mu = 1 + (p^\mu - 1)$$

auf die q^{te} Potenz, so ergiebt sich

(4).
$$\left\{\begin{aligned} \frac{p^{q\mu} - 1}{p^\mu - 1} &= \frac{q}{1} + \frac{q(q-1)}{1.2}(p^\mu - 1) + \cdots \\ &+ \frac{q(q-1)\ldots(q-k+1)}{1.2\ldots k}(p^\mu - 1)^{k-1} + \cdots, \end{aligned}\right.$$

und dieser Ausdruck muss durch λ theilbar sein.

Es bezeichne ϑ einen Primfactor von λ, und zwar sei ϑ^α die höchste in λ enthaltene Potenz von ϑ. Da ϑ in n und folglich in $p^\mu - 1$ aufgeht, so lehrt die Formel (4), dass auch q durch ϑ theilbar ist. Wir behaupten aber ausserdem, dass, wenn ϑ nicht gleich 2 ist, jeder Term des Ausdrucks (4), vom zweiten Terme an, eine höhere Potenz von ϑ enthält, als der erste Term. Das Verhältniss des allgemeinen Terms zum ersten Terme kann nämlich auf folgende Form gebracht werden:

(5).
$$\frac{(q-1)(q-2)\ldots(q-k+1)}{1.2\ldots(k-1)} \times \left(\frac{p^\mu - 1}{\vartheta}\right)^{k-1} \times \frac{\vartheta^{k-1}}{k};$$

die beiden ersten Factoren sind ganze Zahlen; was den dritten Factor betrifft, so ist derselbe grösser als

$$\frac{1 + (k-1)(\vartheta - 1)}{k} \text{ oder als } 1 + \frac{(k-1)(\vartheta - 2)}{k},$$

folglich, da k wenigstens gleich 2 ist, grösser als 1, wenn $\vartheta > 2$ ist. Der mit $\frac{\vartheta^{k-1}}{k}$ gleichbedeutende irreductibele Bruch enthält

daher den Factor ϑ im Zähler. Da das erste Glied der Formel (4) der Voraussetzung nach durch ϑ^α theilbar ist, so muss nach dem Vorhergehenden q den Divisor ϑ^α zulassen.

Ist also λ eine ungerade Zahl, so ist q durch λ theilbar. Wenn umgekehrt q durch λ theilbar ist, so ist dies offenbar auch mit dem Ausdruck (4) der Fall, und folglich ist das erste Glied der Formel (3) eine ganze Zahl. Dann leuchtet ein, dass $q = \lambda$ sein muss, da ν die kleinste Zahl ist, für welche n in $p^\nu - 1$ aufgeht; man hat folglich

$$(6). \qquad \nu = \lambda\mu.$$

Wir wollen jetzt untersuchen, ob wir veranlasst werden, diesen Schluss zu modificiren, wenn λ gerade ist. Wenn λ zunächst das Doppelte einer ungeraden Zahl ist, so muss der Ausdruck (4) und daher auch q durch 2 theilbar sein; damit also der Ausdruck (3) eine ganze Zahl sei, ist auch jetzt noch erforderlich und hinreichend, dass q ein Vielfaches von λ sei, und die Formel (6) bleibt bestehen.

Wir nehmen daher an, λ sei durch eine höhere als die erste Potenz von 2 theilbar. Macht man in dem Ausdruck (5) $\vartheta = 2$, so wird der dritte Factor $\frac{2^{k-1}}{k}$. Da k wenigstens gleich 2 ist, so ist dieser Factor nie kleiner als 1; er reducirt sich aber auf 1 für $k = 2$, und dann kann es vorkommen, dass die beiden ersten Terme des Ausdrucks (4) dieselbe Potenz von 2 enthalten. Dieser Fall tritt jedoch nicht ein, wenn $p^\mu - 1$ durch 4 theilbar ist, d. h. wenn p die Form $4m + 1$ hat, oder wenn p zwar von der Form $4m - 1$, zugleich aber μ eine gerade Zahl ist. In diesen beiden Fällen macht die Anwesenheit des Factor 2 in λ keine Modification unserer Schlüsse erforderlich, und die Formel (6) bleibt bestehen.

Anders verhält es sich in dem Falle, den wir jetzt noch zu erörtern haben, in welchem nämlich λ durch eine höhere als die erste Potenz von 2 theilbar, p von der Form $4m - 1$ und μ eine ungerade Zahl ist; dieser Fall verdient besondere Beachtung. Unserer Voraussetzung nach ist

$$p = 2^i \cdot t - 1 \;,\; \lambda = 2^j \cdot s;$$

darin stellen t und s ungerade Zahlen dar, und die Exponenten

i, j sind gleich 2 oder grösser als 2. Da μ ungerade ist, so liefert die erste dieser Formeln

$$p^\mu = 2^i \vartheta - 1,$$

wo ϑ eine ungerade Zahl ist; da ausserdem, wie wir oben gesehen haben, der Exponent q gerade sein muss, so erhält man, wenn man die letzte Formel auf die q^{te} Potenz erhebt,

$$(7).\ \begin{cases} \dfrac{p^{\mu q} - 1}{p^\mu - 1} = \dfrac{2^{i-1}\vartheta}{2^{i-1}\vartheta - 1}\Big[-\dfrac{q}{1} + \dfrac{q(q-1)}{1.2} 2^i \vartheta - \cdots \\ \qquad + \dfrac{q \ldots (q-k+1)}{1.2 \ldots k} 2^{i(k-1)} \vartheta^{k-1} + \cdots \Big]. \end{cases}$$

Das Verhältniss des allgemeinen Terms zum ersten Terme ist

$$\frac{(q-1)\ldots(q-k+1)}{1.2\ldots(k-1)} \vartheta^{k-1} \times \frac{2^{i(k-1)}}{k}.$$

Nimmt man $k > 1$ an, so ist der letzte Factor dieses Ausdrucks grösser als 1, da i wenigstens 2 ist, und der irreductibele Bruch, welcher diesem Factor gleich ist, hat einen geraden Zähler; ausserdem sind die übrigen Factoren ganze Zahlen; folglich enthält in der Formel (7) der erste der eingeklammerten Terme eine nicht so hohe Potenz von 2, als die folgenden Terme. Bezeichnet man dann mit ω die kleinste Anzahl von Factoren 2, die man in q einführen muss, damit der Ausdruck (3) ganz werde, so hat man

$$\omega = 1, \text{ oder } \omega = j - i + 1,$$

nämlich $\omega = 1$, wenn $j <$ oder $= i$ ist, denn in diesem Falle genügt es, dass q gerade sei, und

$$\omega = j - i + 1, \text{ wenn } j > i \text{ ist.}$$

Ausserdem darf q in beiden Fällen nur die ungeraden Primfactoren von λ enthalten; es ist daher

$$q = \frac{\lambda}{2^{j-1}}, \text{ oder } q = \frac{\lambda}{2^{i-1}},$$

und folglich

$$(8).\qquad \nu = \frac{\lambda\mu}{2^{j-1}},$$

oder

$$(9).\qquad \nu = \frac{\lambda\mu}{2^{i-1}}.$$

Die Formel (8) findet statt, wenn $j < i$, die Formel (9), wenn $j > i$ ist; für $i = j$ fallen beide Formeln zusammen.

356. Wir wollen jetzt die Folgen der vorhergehenden Untersuchung entwickeln. Zunächst betrachten wir den Fall, in welchem die Formel (6) besteht, und bezeichnen mit N die Anzahl der irreductibelen ganzen Functionen ν^{ten} Grades, welche zum Exponenten n gehören. Nach No. 352 ist

$$N = \frac{\varphi(n)}{\nu} = \frac{\varphi(n)}{\lambda\mu},$$

oder, der Formel (2) wegen,

$$N = \frac{1}{\mu} : \frac{p^\mu - 1}{d} \cdot \frac{\varphi(n)}{n}.$$

Ist nun n' eine Zahl, welche alle Primfactoren von n mit irgend welchen Exponenten, ausserdem aber keine anderen Primfactoren enthält, so hat man

$$\frac{\varphi(n')}{n'} = \frac{\varphi(n)}{n},$$

und da $\frac{p^\mu - 1}{d}$ der grösste gemeinschaftliche Divisor von n und $p^\mu - 1$ ist, so kann man

$$n' = \frac{p^\mu - 1}{d}$$

nehmen. Wird n durch diesen Werth n' ersetzt, so geht der Ausdruck von N über in

$$(10). \qquad N = \frac{1}{\mu}\,\varphi\left(\frac{p^\mu - 1}{d}\right),$$

und daraus folgt, dass N auch die Anzahl der irreductibelen Functionen μ^{ten} Grades darstellt, welche zum Exponenten $\frac{p^\mu - 1}{d}$ gehören.

Wir setzen der Kürze wegen

$$\frac{p^\mu - 1}{d} = \delta,$$

so dass $n = \delta\lambda$ ist, und zerlegen $x^\delta - 1$ in Factoren, die nach dem Modul p irreductibel sind; es ergebe sich

$$(11). \qquad x^\delta - 1 = F(x)\,F_1(x)\,F_2(x) \ldots + p\chi(x).$$

μ ist die kleinste Zahl von der Beschaffenheit, dass $x^{p^\mu - 1} - 1$ durch $x^\delta - 1$ nach dem Modul p theilbar ist; denn wenn $\mu' < \mu$ wäre, und δ in $p^{\mu'} - 1$ aufginge, so müsste die Zahl $p^{\mu'} - 1$ alle Primfactoren von n enthalten, was der Voraussetzung widerspricht. Diese Bemerkung bestätigt die Thatsache, die übrigens

aus unserer Analyse hervorgeht, dass der Grad jedes irreductibelen Factors der Formel (11) gleich μ oder gleich einem Divisor von μ ist.

Wird jetzt in der Formel (11) x durch x^λ ersetzt, so folgt

(12). $$x^n - 1 = F(x^\lambda)\; F_1(x^\lambda)\; F_2(x^\lambda) \cdots + p\chi(x^\lambda).$$

Sind

(13). $$F(x)\;,\; F_1(x)\;,\; \ldots\;,\; F_{N-1}(x)$$

die N Factoren μ^{ten} Grades der Formel (11), so sind in (12) die Factoren vom Grade $\lambda\mu = \nu$ offenbar

(14). $$F(x^\lambda)\;,\; F_1(x^\lambda)\;,\; \ldots\;,\; F_{N-1}(x^\lambda).$$

Nun giebt es N irreductibele Functionen ν^{ten} Grades, welche nach dem Modul p in $x^n - 1$ aufgehen; diese Functionen sind daher nichts Anderes, als die Polynome (14), und wir erhalten den folgenden Satz:

Lehrsatz I. — Hat man die N nach dem Modul p irreductibelen ganzen Functionen μ^{ten} Grades gebildet, welche zum Exponenten $\frac{p^\mu - 1}{d}$ gehören, und ersetzt sodann x durch x^λ, wo λ eine Zahl bedeutet, die prim zu d ist, und die keinen nicht auch in $p^\mu - 1$ aufgehenden Primfactor enthält, so erhält man die N irreductibelen Functionen vom Grade $\lambda\mu$, welche zum Exponenten $\lambda\,\frac{p^\mu - 1}{d}$ gehören. Eine Ausnahme macht jedoch der Fall, in welchem μ eine ungerade und λ eine durch 4 theilbare Zahl ist, während zugleich p die Form $4i - 1$ hat.

357. Fassen wir jetzt diesen Ausnahmefall in's Auge: p hat die Form $4m - 1$, μ ist ungerade und λ eine durch 4 theilbare Zahl. Dann findet eine der Formeln (8) und (9) statt, und wenn wieder N die Anzahl der irreductibelen ganzen Functionen ν^{ten} Grades bezeichnet, die zum Exponenten n gehören, und k die kleinste der beiden Zahlen i und j darstellt, so hat man

$$N = \frac{\varphi(n)}{\nu} = 2^{k-1}\,\frac{\varphi(n)}{\lambda\mu}.$$

Der Formel (2) wegen kann man auch schreiben:

$$N = 2^{k-1}\,\frac{1}{\mu}\cdot\frac{p^\mu - 1}{d}\cdot\frac{\varphi(n)}{n}.$$

Da alle Primfactoren einer der Zahlen n und $\frac{p^\mu - 1}{d}$ auch der andern angehören, so kann man hier

$$\frac{p^\mu - 1}{d} \quad \frac{\varphi(n)}{n}$$

durch $\varphi\left(\frac{p^\mu - 1}{d}\right)$ ersetzen und erhält

$$N = 2^{k-1} \frac{1}{\mu} \varphi\left(\frac{p^\mu - 1}{d}\right).$$

$\frac{N}{2^{k-1}}$ ist daher die Anzahl der irreductibelen Functionen μ^{ten} Grades, welche zum Exponenten $\frac{p^\mu - 1}{d} = \delta$ gehören.

Wir behalten die Formel (11), welche die Zerlegung des Binoms $x^\delta - 1$ in irreductibele Factoren liefert, und ebenso die Formel (12) bei, welche aus (11) dadurch hervorgeht, dass man x durch x^λ ersetzt. Diejenigen der Factoren $F(x)$, $F_1(x)$, ..., welche zu einem Exponenten gehören, der kleiner als δ ist, liefern in (12) entsprechende Factoren, deren irreductibele Divisoren zu einem Exponenten gehören, der kleiner als n ist. Die irreductibelen Factoren von $x^n - 1$, welche zum Exponenten $\nu = \frac{\lambda\mu}{2^{k-1}}$ gehören, müssen daher in eins der $\frac{N}{2^k - 1}$ Polynome

$$F(x^\lambda)\ ,\ F_1(x^\lambda)\ ,\ F_2(x^\lambda)\ ,\ \ldots$$

aufgehen, welche den auf den Exponenten δ bezüglichen $\frac{N}{2^k - 1}$ Factoren

$$F(x)\ ,\ F_1(x)\ ,\ F_2(x)\ ,\ \ldots$$

entsprechen. Die Polynome, um die es sich handelt, sind vom Grade $\lambda\mu$, ihre Anzahl ist $\frac{N}{2^k - 1}$, und die Anzahl der irreductibelen Functionen vom Grade $\frac{\lambda\mu}{2^{k-1}}$ ist N. Jedes unserer Polynome ist folglich das Produkt von 2^{k-1} irreductibelen Factoren $\left(\frac{\lambda\mu}{2^k - 1}\right)^{\text{ten}}$ Grades. Daraus entnehmen wir folgenden Satz:

Lehrsatz II. — Es sei p eine Primzahl von der Form $2^i t - 1$, wo i nicht kleiner als 2 und t eine ungerade Zahl ist; ferner seien μ eine ungerade Zahl, $\frac{p^\mu - 1}{d}$ ein Divisor von $p^\mu - 1$, λ eine Zahl von der Form $2^j s$,

wo j nicht kleiner als 2 und s ungerade ist; endlich sei k die kleinste der Zahlen i und j.

Hat man die $\frac{N}{2^{k-1}}$ nach dem Modul p irreductibelen ganzen Functionen μ^{ten} Grades gebildet, welche zum Exponenten $\frac{p^\mu - 1}{d}$ gehören, und ersetzt darin x durch die Potenz x^λ, deren Exponent $\lambda = 2^j s$ prim zu d ist und nur die in $p^\mu - 1$ aufgehenden Primfactoren enthält, so erhält man $\frac{N}{2^{k-1}}$ Functionen vom Grade $\lambda\mu$, und jede derselben ist in 2^{k-1} irreductibele Factoren zerlegbar, so dass sich im Ganzen N irreductibele Polynome vom Grade $\frac{\lambda\mu}{2^{k-1}}$ ergeben.

358. Wir bezeichnen mit g eine primitive Wurzel der Primzahl p. Die Functionen ersten Grades, welche zum Exponenten $\frac{p-1}{d}$ gehören, sind offenbar $x - g^{\alpha d}$, wenn α eine Zahl bedeutet, die prim zu $\frac{p-1}{d}$ ist. Stellt man also diese Functionen durch $x - g^e$ dar, so ist d der grösste gemeinschaftliche Divisor der Zahlen e und $p-1$. Wird jetzt in den Lehrsätzen I und II $\mu = 1$ vorausgesetzt, so ergiebt sich der folgende neue Satz, der von grosser Wichtigkeit ist:

Lehrsatz III. — Es seien g eine primitive Wurzel der Primzahl p; λ eine ganze Zahl, welche keinen nicht auch in $p-1$ aufgehenden Primfactor enthält; e eine ganze Zahl, die prim zu λ ist; d der grösste gemeinschaftliche Divisor der Zahlen e und $p-1$.

1⁰. Wenn p von der Form $4q+1$ ist, oder wenn p die Form $4q-1$ hat, zugleich aber λ ungerade oder das Doppelte einer ungeraden Zahl ist, so ist die binomische Function $x^\lambda - g^e$ nach dem Modul p irreductibel und gehört zum Exponenten $\lambda \frac{p-1}{d}$.

2⁰. Wenn p und λ beziehungsweise die Formen

$$p = 2^i t - 1\ ,\ \lambda = 2^j s$$

haben, wo i und j wenigstens gleich 2, und t, s ungerade Zahlen sind, und wenn ausserdem die kleinste der Zahlen i, j mit k bezeichnet wird, so ist die bino-

mische Function $x^\lambda - g^e$ nach dem Modul p reductibel, und zwar lässt sie sich in 2^{k-1} irreductibele Factoren vom Grade $\frac{\lambda}{2^{k-1}}$ zerlegen, welche sämmtlich zum Exponenten $\lambda\frac{p-1}{d}$ gehören.

Dieser Satz lehrt uns alle nach dem Primzahlmodul p irreductibelen binomischen Functionen, ohne Ausnahme, kennen. Die Function $x^\lambda - g^e \ (mod.\ p)$ kann nämlich nicht irreductibel sein, wenn λ und e einen Divisor gemeinschaftlich haben. Wenn ausserdem λ einen Primfactor ϑ enthält, der nicht in $p-1$ aufgeht, so besitzt die Congruenz $x^\vartheta - g^e \equiv 0 \ (mod.\ p)$ eine Wurzel, und folglich lässt $x^\vartheta - g^e$ nach dem Modul p einen Divisor von der Form $x - \alpha$ zu; daraus geht hervor, dass auch $x^{\frac{\lambda}{\vartheta}} - \alpha$ ein Divisor von $x^\lambda - g^e$ sein wird.

359. Wenn p die Form $2^i t - 1$ hat, wo i wenigstens gleich 2 und t eine ungerade Zahl ist, so giebt es, wie wir soeben gesehen haben, nur dann irreductibele binomische Functionen vom Grade λ, wenn λ ungerade oder das Doppelte einer ungeraden Zahl ist. Man kann jedoch sehr leicht, auch wenn λ eine beliebige gerade Zahl ist, nach dem Modul p irreductibele trinomische Functionen vom Grade λ bilden, vorausgesetzt, dass λ nur die Primfactoren enthält, durch welche $p-1$ theilbar ist.

Der Voraussetzung nach hat p die Form

$$p = 2^i t - 1,$$

und darin ist t eine ungerade Zahl. Setzen wir

$$\nu = 2^{i-1}\lambda,$$

so ist die Zahl ν durch 2^i theilbar, da λ gerade ist. Bezeichnet sodann g eine primitive Wurzel von p und e eine Zahl, die prim zu λ ist, so lässt sich die Function

$$x^\nu - g^e$$

nach dem Lehrsatz III (No. 358) in 2^{i-1} irreductibele Factoren vom Grade λ zerlegen. Um diese Factoren zu erhalten, bemerken wir, dass die Zahlen 2^i und $p-1$ den grössten gemeinschaftlichen Divisor 2 haben, und dass e und $\frac{p-1}{2}$ ungerade sind; daraus folgt, dass man stets zwei ganze Zahlen ϑ und ζ von der Beschaffenheit ermitteln kann, dass

$$2^i \vartheta - (p-1)\zeta = e + \frac{p-1}{2}$$

ist; dann hat man

$$g^{2^i \vartheta} \equiv - g^e \ (mod.\ p),$$

und die Function, die wir betrachten, ist

$$x^\nu - g^c \equiv x^{2^{i-1}\lambda} + g^{2^i\vartheta} \ (mod.\ p).$$

Dies vorausgesetzt, mögen u und v zwei Veränderliche bezeichnen. Da t und $\frac{p-1}{2}$ ungerade Zahlen sind, so ist die erste der beiden Functionen

$$u^{\frac{p+1}{2}} + v^{\frac{p+1}{2}}, \quad u^{\frac{p-1}{2}} + v^{\frac{p-1}{2}}$$

durch $u^{2^{i-1}} + v^{2^{i-1}}$, die zweite durch $u + v$ algebraisch theilbar. Das Produkt dieser Functionen lässt sich daher auf die Form

$$(u+v)\,(u^{2^{i-1}} + v^{2^{i-1}})\, f(u, v)$$

bringen, wo f ein Polynom mit ganzen Coefficienten ist. Vollführt man aber die Multiplication beider Functionen, so erhält man

$$(u^p + v^p) + (u+v)\,(uv)^{\frac{p-1}{2}};$$

ausserdem ist bekanntlich

$$(u^p + v^p) = (u+v)^p + p\chi(u, v),$$

und es leuchtet ein, dass $\chi(u, v)$ durch $u+v$ theilbar ist. Man kann folglich schreiben

$$(u^p + v^p) = (u+v)^p - p\,(u+v)\, f_1(u, v),$$

und darin stellt f_1 ein Polynom mit ganzen Coefficienten dar. Setzt man die beiden Ausdrücke, die wir für das betrachtete Produkt erhalten haben, einander gleich, so ergiebt sich, wenn der Factor $u+v$ unterdrückt wird, die folgende Identität:

$$(1).\quad (u+v)^{p-1} + (uv)^{\frac{p-1}{2}} = (u^{2^{i-1}} + v^{2^{i-1}})\, f(u,v) + pf_1(u,v);$$

darin sind f und f_1 offenbar ganze und symmetrische Functionen der Veränderlichen u und v, mit ganzen Coefficienten.

Wir ersetzen jetzt u und v durch die beiden Wurzeln der Gleichung

$$X^2 - \xi X - 1 = 0,$$

in welcher ξ eine neue Veränderliche bezeichnet. Alle ganzen und symmetrischen Functionen von u und v, mit ganzen Coefficien-

ten, werden dann ganze Functionen von ξ, deren Coefficienten gleichfalls ganz sind, und die Formel (1) liefert

(2). $$\xi^{p-1} - 1 = E(\xi)\,\varphi(\xi) + p\chi(\xi),$$

wenn

$$E(\xi) = u^{2^{i-1}} + v^{2^{i-1}},$$

oder

(3). $$E(\xi) = \left[\frac{\xi}{2} + \sqrt{\frac{\xi^2}{4} + 1}\right]^{2^{i-1}} + \left[\frac{\xi}{2} - \sqrt{\frac{\xi^2}{4} + 1}\right]^{2^{i-1}}$$

gesetzt wird, und wenn $\varphi(\xi)$, $\chi(\xi)$ Polynome mit ganzen Coefficienten bezeichnen.

Da jetzt das Polynom $E(\xi)$ ein Divisor von

$$\xi^{p-1} - 1 - p\chi(\xi)$$

ist, so besitzt die Congruenz

(4). $$E(\xi) \equiv 0 \pmod{p},$$

deren Grad 2^{i-1} ist, 2^{i-1} Wurzeln. Werden diese Wurzeln mit

$$\xi_1, \xi_2, \ldots, \xi_{2^{i-1}}$$

bezeichnet, so hat man

(5). $$E(\xi) = (\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_{2^{i-1}}) + p\omega(\xi),$$

und darin ist $\omega(\xi)$ ein Polynom mit ganzen Coefficienten.

Die Formeln (3) und (5) liefern für $E(\xi)$ Werthe, die identisch sein müssen. Setzt man diese Werthe einander gleich und macht

$$\xi = \frac{x^{\frac{\lambda}{2}}}{g^\vartheta} - \frac{g^\vartheta}{x^{\frac{\lambda}{2}}},\quad \sqrt{\xi^2 + 4} = \frac{x^{\frac{\lambda}{2}}}{g^\vartheta} + \frac{g^\vartheta}{x^{\frac{\lambda}{2}}},$$

so folgt nach Fortschaffung der Nenner

$$x^{2^{i-1}\lambda} + g^{2^i\vartheta} = \Pi\left(x^\lambda - \xi g^\vartheta x^{\frac{\lambda}{2}} - g^{2\vartheta}\right) + p\,\Phi(x);$$

$\Phi(x)$ bezeichnet ein Polynom mit ganzen Coefficienten, und das Zeichen Π drückt das Produkt der Factoren aus, welche der Ausdruck

$$x^\lambda - \xi g^\vartheta x^{\frac{\lambda}{2}} - g^{2\vartheta}$$

darstellt; wenn für ξ jede Wurzel der Congruenz (4) gesetzt wird. Diese Factoren sind die irreductibelen Functionen, die wir ermitteln wollten.

Ueber eine nach dem Modul p irreductibele Function p^{ten} Grades.

360. Die in No. 351 auseinandergesetzte Methode zur Bildung der irreductibelen Functionen ist wenig geeignet, angewandt zu werden. Von grosser praktischer Bedeutung sind dagegen die vorhergehenden Lehrsätze, die es ermöglichen, direkt eine irreductibele Function vom Grade λ zu bilden, wenn λ nur die Primfactoren des um eine Einheit verringerten Moduls enthält. Wir werden nämlich später sehen, dass die Kenntniss einer einzigen, nach einem Primzahlmodul irreductibelen Function irgend eines Grades ausreicht, um alle übrigen irreductibelen Functionen desselben Grades direkt zu bilden.

Wir theilen noch einen Satz mit, der eine nach dem Primzahlmodul p irreductibele Function p^{ten} Grades kennen lehrt.

Lehrsatz. — Wenn die Zahl g nicht durch die Primzahl p theilbar ist, so ist die Function $x^p - x - g$ in Beziehung auf den Modul p irreductibel.

Es sei nämlich $F(x)$ ein nach dem Modul p irreductibeler Factor der in Rede stehenden Function; dann ist

$$x^p - x - g \equiv F(x) \cdot \varphi(x) \pmod{p},$$

und darin bezeichnet $\varphi(x)$ ein Polynom mit ganzen Coefficienten. Daraus folgt

$$x^p \equiv x + g + F(x)\,\varphi(x) \pmod{p}$$

und, wenn beide Glieder auf die $(p^{m-1})^{\text{te}}$ Potenz erhoben werden,

$$x^{p^m} \equiv x^{p^{m-1}} + g + F(x)\,\varphi(x) \pmod{p};$$

auch in dieser Formel ist $\varphi(x)$ ein Polynom mit ganzen Coefficienten. Macht man der Reihe nach $m = 1, 2, 3, \ldots,$ so ergiebt sich

$$\left.\begin{array}{lll} x^p \equiv x + g + F(x)\,\varphi(x) & & \\ x^{p^2} \equiv x^p + g + F(x)\,\varphi(x) & \equiv & x + 2g + F(x)\,\varphi(x) \\ x^{p^3} \equiv x^{p^2} + g + F(x)\,\varphi(x) & \equiv & x + 3g + F(x)\,\varphi(x) \\ \cdots & \cdots & \cdots \end{array}\right\} \pmod{p},$$

und man erhält für jeden Werth von m

$$x^{p^m} \equiv x + mg + F(x)\,\varphi(x) \pmod{p}.$$

Wir setzen jetzt voraus, m bezeichne den Grad von $F(x)$;

dann geht $F(x)$ in $x^{p^m} - x$ auf; mithin fordert die vorhergehende Formel, dass

$$mg \equiv 0 \text{ oder } m \equiv 0 \pmod{p}$$

sei. Da also m ein Vielfaches von p ist, so muss $m = p$ sein, d. h. $F(x)$ ist nichts Anderes, als die Function $x^p - x - g$ selbst.

Classification der in Beziehung auf einen Primzahlmodul und eine irreductibele Function reducirten Functionen.

361. Es sei $F(x)$ eine nach dem Primzahlmodul p irreductibele ganze Function. Setzt man

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{\nu-1} x^{\nu-1},$$

wo $a_0, a_1, \ldots, a_{\nu-1}$ ganze Zahlen sind, die zwischen 0 und $p-1$, oder zwischen $-\frac{p-1}{2}$ und $+\frac{p-1}{2}$ liegen, so ist $f(x)$ der allgemeine Ausdruck der nach dem Modul p und nach der irreductibelen Function $F(x)$ reducirten Functionen. Die Gesammtzahl dieser reducirten Functionen ist p^ν, und jede derselben genügt, wie wir gesehen haben, der Bedingung

$$[f(x)]^{p^\nu} - f(x) \equiv F(x)\,\psi(x) \pmod{p},$$

welche ausdrückt, dass die Function

$$[f(x)]^{p^\nu} - f(x)$$

nach dem Modul p durch $F(x)$ theilbar ist.

Im vorigen Kapitel haben wir eine Eintheilung der ganzen Zahlen gegeben; eine ganz ähnliche Eintheilung wollen wir jetzt in Betreff der Functionen $f(x)$ begründen. Die nachstehende Entwicklung setzt den Lehrsatz, den wir uns soeben in's Gedächtniss zurückriefen, nicht voraus; derselbe wird im Gegentheil sich leicht aus dieser Entwicklung entnehmen lassen.

Wir werden in der Folge eine besondere Bezeichnung in Anwendung bringen, deren Einführung in die vorliegende Theorie uns von Nutzen zu sein scheint. Da wir nämlich $A \equiv B \pmod{p.}$ schreiben, um auszudrücken, dass die Differenz der Zahlen A und B durch p theilbar ist, so ist es naturgemäss, sich der Bezeichnung

$$\mathfrak{F}(x) \equiv f(x)\ [mod.\ p,\ F(x)]$$

zu bedienen, um auszudrücken, dass die Differenz der beiden ganzen Functionen $\mathfrak{F}(x)$, $f(x)$ nach dem Modul p durch die irreductibele Function $F(x)$ theilbar ist. Letztere nennen wir dann die Modularfunction und sagen: $\mathfrak{F}(x)$ und $f(x)$ sind nach dem Modul p und nach der Modularfunction $F(x)$ congruent. Endlich werden wir der Kürze wegen den nach dem Modul und nach der Modularfunction reducirten Functionen den Namen kleinste Reste beilegen.

362. Dies vorausgesetzt, sei X irgend einer der $p^\nu - 1$ von Null verschiedenen Werthe von $f(x)$; wir nehmen im Folgenden auf den Werth Null überhaupt keine Rücksicht. Die kleinsten Reste der Terme der Reihe

$$1\,,\ X\,,\ X^2\,,\ X^3\,,\ \ldots$$

sind gleichfalls Werthe von $f(x)$. Da aber $f(x)$ nur $p^\nu - 1$ verschiedene Werthe hat, so müssen einige dieser Werthe sich unendlich oft in der Reihe der Potenzen von X vorfinden. Wir nehmen an, es sei

$$X^{n+n'} \equiv X^{n'} \ [mod.\ p,\ F(x)]\,,$$

oder

$$X^{n'}\,(X^n - 1) \equiv 0\ [mod.\ p,\ F(x)]\,.$$

Da $X^{n'}$ nach dem Modul p nicht durch $F(x)$ theilbar sein kann, so muss

$$X^n \equiv 1\ [mod.\ p,\ F(x)]\,,$$

und folglich

$$X^{2n} \equiv 1\,,\ X^{3n} \equiv 1\,,\ \ldots\ [mod.\ p,\ F(x)]$$

sein. Es giebt daher eine unendliche Menge Potenzen von X, welche der Einheit congruent sind. Bezeichnet n die kleinste Zahl, für welche

$$X^n \equiv 1\ [mod.\ p,\ F(x)]$$

ist, so stellen

$$(1).\qquad 1\,,\ X\,,\ X^2\,,\ X^3\,,\ \ldots\,,\ X^{n-1}$$

n Werthe von $f(x)$ dar, deren kleinste Reste verschieden sind. Hat man $p^\nu - 1 = n$, so umfasst die Reihe (1), oder die Reihe der kleinsten Reste von (1) alle Werthe von $f(x)$.

Wenn $p^\nu - 1 > n$ ist, so sei X_1 einer der Werthe von $f(x)$, welche nicht unter den kleinsten Resten der Reihe (1) ent-

halten sind. Multiplicirt man die Functionen (1) mit X_1, so erhält man die neuen Functionen

(2). $$X_1\,,\ XX_1\,,\ X^2X_1\,,\ \ldots\,,\ X^{n-1}X_1\,,$$

deren kleinste Reste verschieden sind. Es seien nämlich n' und n'' zwei zwischen 0 und n liegende Zahlen; hätte man nun

$$X^{n'}X_1 - X^{n''}X_1 \equiv 0\ [mod.\ p,\ F(x)]\,,$$

so müsste, da X_1 nach dem Modul p nicht durch $F(x)$ theilbar sein kann,

$$X^{n'} - X^{n''} \equiv 0\ [mod.\ p,\ F(x)]$$

sein, was der Voraussetzung widerspricht. Ausserdem sind die Grössen (2) von den Termen der Reihe (1) verschieden; denn wäre z. B.

$$X^{n'}X_1 \equiv X^{n''}\ [mod.\ p,\ F(x)],$$

so würde sich durch Multiplication mit $X^{n-n'}$

$$X^nX_1 \equiv X^{n-n'+n''} \text{ oder } X_1 \equiv X^{n-n'+n''}\ [mod.\ p,\ F(x)]$$

ergeben, was mit der Voraussetzung gleichfalls in Widerspruch steht.

Wir sehen somit, dass $p^\nu - 1$ entweder gleich $2n$, oder grösser als $2n$ ist. Wenn $p^\nu - 1 > 2n$ ist, so sei X_2 ein Werth von $f(x)$, welcher sich unter den kleinsten Resten von (1) und (2) nicht vorfindet. Multiplicirt man die Functionen (1) mit X_2, so erhält man die neuen Functionen

(3). $$X_2\,,\ XX_2\,,\ X^2X_2\,,\ \ldots\,,\ X^{n-1}X_2\,,$$

und man überzeugt sich durch Wiederholung des eben dargelegten Schlussverfahrens, dass die kleinsten Reste der Functionen (3) untereinander und von den Resten der Reihe (1) verschieden sind. Es ist auch leicht einzusehen, dass kein Term von (3) denselben kleinsten Rest wie ein Term der Reihe (2) haben kann; hätte man z. B.

$$X^{n'}X_2 \equiv X^{n''}X_1\ [mod.\ p,\ F(x)]\,,$$

so würde sich durch Multiplication mit $X^{n-n'}$

$$X^nX_2 \equiv X^{n-n'+n''}X_1 \text{ oder } X_2 \equiv X^{n-n'+n''}X_1\ [mod.\ p,\ F(x)]$$

ergeben, was der Voraussetzung widerspricht.

$p^\nu - 1$ ist danach entweder $= 3n$, oder $> 3n$. So fort-

fahrend erkennt man, dass $p^\nu - 1$ jedenfalls ein Vielfaches von n ist.

Wenn n die kleinste Zahl ist, für welche man

$$X^n \equiv 1 \; [mod.\ p,\ F(x)]$$

hat, so sagen wir: Die Function X gehört nach dem Modul p und nach der Modularfunction $F(x)$ zum Exponenten n. Da diese Zahl n ein Divisor von $p^\nu - 1$ ist, so zieht die vorhergehende Congruenz die folgende nach sich:

$$X^{p^\nu - 1} - 1 \equiv 0 \; [mod.\ p,\ F(x)],$$

und wir haben somit den in No. 346 hergeleiteten Satz auf's Neue bewiesen.

363. Lehrsatz I. — Wenn die nach dem Modul p irreductibele Function $F(x)$ vom Grade ν ist, und wenn n irgend einen Divisor von $p^\nu - 1$ bezeichnet, so giebt es so viele reducirte Functionen, welche nach dem Doppelmodul $[p, F(x)]$ zum Exponenten n gehören, als die Zahl $\varphi(n)$ Einheiten enthält; $\varphi(n)$ drückt aus, wie viele Zahlen prim zu n und nicht grösser als n sind.

Der Beweis dieses Satzes ist mit demjenigen identisch, den wir in No. 306 anwandten, als die Aufgabe vorlag, die ganzen Zahlen in Beziehung auf einen Primzahlmodul zu classificiren. Der Wichtigkeit des Gegenstandes wegen werden wir ihn aber nochmals vorführen.

Wir nehmen an, es gebe eine zum Exponenten n gehörende Function X_1; dann sind die kleinsten Reste der Functionen

$$(1). \qquad 1,\ X_1,\ X_1^2,\ \ldots,\ X_1^{n-1}$$

von einander verschieden. Bezeichnet ausserdem e irgend eine der Zahlen

$$1,\ 2,\ 3,\ \ldots,\ (n-1),$$

so zieht die Congruenz

$$X_1^n \equiv 1 \; [mod.\ p,\ F(x)]$$

die folgende nach sich:

$$(2). \qquad X_1^{ne} \equiv 1 \text{ oder } (X_1^e)^n \equiv 1 \; [mod.\ p,\ F(x)].$$

Setzt man also in

$$X^n \equiv 1$$

an die Stelle von X jede der n Functionen (1), so erhält man

n Resultate, die nach dem Modul p durch $F(x)$ theilbar sind; nach dem Satze der No. 345 giebt es daher ausser den Resten der Functionen (1) keine reducirte Function, deren n^{te} Potenz nach dem Modul p durch $F(x)$ theilbar wäre.

Wir bezeichnen jetzt mit m den Exponenten, zu welchem X_1^e gehört, d. h. die kleinste Zahl, für welche

$$(3). \qquad (X_1^e)^m = X_1^{me} \equiv 1 \; [mod. \, p, F(x)]$$

ist. Die Congruenz (2) fordert, dass n ein Vielfaches von m sei; da umgekehrt X_1 zum Exponenten n gehört, so muss der Congruenz (3) wegen me ein Vielfaches von n, oder, wenn e prim zu n ist, m durch n theilbar sein. Man hat also, e als prim zu n vorausgesetzt, $m = n$, d. h. X_1^e gehört zum Exponenten n, wenn e prim zu n ist. Haben aber n und e einen gemeinschaftlichen Divisor $\vartheta > 1$, so ist

$$(X_1^e)^{\frac{n}{\vartheta}} = (X_1^{\frac{e}{\vartheta}})^n \equiv 1 \; [mod. \, p, F(x)],$$

und folglich gehört X_1^e nicht zum Exponenten n. Wenn es daher überhaupt reducirte Functionen giebt, die zum Exponenten n gehören, so muss die Anzahl derselben gleich $\varphi(n)$ sein.

Nun gehört aber jede reducirte Function zu einem Exponenten, welcher einer der Divisoren

$$d \, , \, d' \, , \, d'' \, \ldots$$

von $p^\nu - 1$ ist. Bezeichnet also $\psi(n)$ die Anzahl der zum Exponenten n gehörenden reducirten Functionen, so hat man

$$\psi(d) + \psi(d') + \psi(d'') + \cdots = p^\nu - 1,$$

mithin auch

$$\psi(d) + \psi(d') + \psi(d'') + \cdots = \varphi(d) + \varphi(d') + \varphi(d'') + \cdots.$$

Wir haben aber oben gefunden, dass entweder

$$\psi(n) = \varphi(n) \, , \text{ oder } \psi(n) = 0$$

ist; der letztere Fall kann der vorhergehenden Formel wegen niemals stattfinden, und es ist somit

$$\psi(n) = \varphi(n).$$

Zusatz. — Es giebt $\varphi(p^\nu - 1)$ reducirte Functionen, welche nach dem Modul p und der Modularfunction $F(x)$ zum Exponenten $p^\nu - 1$ gehören.

364. Lehrsatz II. — Wenn zwei reducirte Functionen X_1, X_2 in Beziehung auf den Modul p und die Modu-

larfunction $F(x)$ zu Exponenten n_1, n_2 gehören, die prim zu einander sind, so gehört der kleinste Rest des Products $X_1 X_2$ zum Exponenten $n_1 n_2$.

Es sei nämlich s ein Exponent, für welchen die Congruenz

$$(1). \qquad (X_1 X_2)^s = X_1^s X_2^s \equiv 1 \ [mod.\ p,\ F(x)]$$

besteht. Wird diese Congruenz auf die n_1^{te} Potenz erhoben, so ergiebt sich

$$X_1^{sn_1} X_2^{sn_1} \equiv 1 \ [mod.\ p,\ F(x)],$$

oder, da X_1 zum Exponenten n_1 gehört,

$$(2). \qquad X_2^{sn_1} \equiv 1 \ [mod.\ p,\ F(x)].$$

Die Congruenz (2) zeigt, dass sn_1 ein Vielfaches von n_2 ist; n_1 und n_2 sind aber relative Primzahlen; folglich ist s durch n_2 theilbar. Ausserdem ist n_2 irgend eine der beiden Zahlen n_1, n_2; mithin ist s sowohl durch n_1, als auch durch n_2, d. h. s ist durch das Produkt $n_1 n_2$ theilbar. Da endlich der Congruenz (1) genügt wird, wenn man $s = n_1 n_2$ nimmt, so sieht man, dass $n_1 n_2$ in der That der Exponent ist, zu welchem das Produkt $X_1 X_2$ gehört.

Zusatz I. — Wenn die reducirten Functionen

$$X_1,\ X_2,\ \ldots,\ X_i$$

in Beziehung auf den Modul p und die Modularfunction $F(x)$ zu Exponenten $n_1, n_2, \ldots, n_i$ gehören, von denen je zwei prim zu einander sind, so gehört der kleinste Rest der Function $X_1 X_2 \ldots X_i$ zum Exponenten $n_1 n_2 \ldots n_i$.

Zusatz II. — Wenn die Zahl $p^\nu - 1$ gleich $2^\varrho q^\lambda r^\mu \ldots$ ist, wo $q, r, \ldots$ ungleiche ungerade Primzahlen sind, und wenn $X_0, X_1, X_2, \ldots$ reducirte Functionen bezeichnen, die beziehungsweise zu den Exponenten $2^\varrho, q^\lambda, r^\mu, \ldots$ gehören, so gehört das Produkt $X_0 X_1 X_2 \ldots$ oder sein kleinster Rest zum Exponenten $p^\nu - 1$.

Congruenzen nach einem Primzahlmodul und nach einer Modularfunction.

365. Es sei $\mathfrak{F}(X)$ eine ganze Function der Veränderlichen X, in welcher die Coefficienten der Potenzen von X ganze Zah-

len oder in Beziehung auf den Modul p und die irreductibele Function ν^{ten} Grades $F(x)$ genommene ganze Functionen der Veränderlichen x sind. Wir nennen den Werth

$$X = f(x)$$

eine Wurzel der Congruenz

$$\mathfrak{F}(X) \equiv 0 \; [mod.\; p,\; F(x)],$$

wenn nach Einsetzung von $f(x)$ an die Stelle von X die Function $\mathfrak{F}(X)$ in Beziehung auf den Modul p durch $F(x)$ theilbar ist.

Mit Rücksicht hierauf lässt sich der Zusatz zu dem in No. 345 bewiesenen Satze folgendermassen aussprechen:

Eine in Beziehung auf einen Primzahlmodul und eine irreductibele Function genommene Congruenz hat höchstens so viele Wurzeln, als ihr Grad Einheiten enthält.

366. Lehrsatz I. — Es seien $F(x)$ und $\mathfrak{F}(x)$ zwei nach dem Modul p irreductibele Functionen, und zwar sei $F(x)$ vom Grade ν, während der Grad von $\mathfrak{F}(x)$ gleich ν oder gleich einem Divisor von ν ist: Dann hat die Congruenz

$$\mathfrak{F}(X) \equiv 0 \; [mod.\, p,\, F(x)]$$

genau so viele Wurzeln, als ihr Grad Einheiten enthält.

Da nämlich der Grad von $\mathfrak{F}(X)$ ein Divisor von ν ist, so hat man

$$X^{p^\nu} - X = \mathfrak{F}(X)\,\mathfrak{F}_1(X) + p\chi(X),$$

wo $\mathfrak{F}_1(X)$ und $\chi(X)$ Polynome mit ganzen Coefficienten sind. Andererseits hat die Congruenz

$$X^{p^\nu} - X \equiv 0 \; [mod.\; p,\; F(x)]$$

die p^ν reducirten Functionen von x, Null nicht ausgeschlossen, zu Wurzeln, und jede dieser Wurzeln gehört einer der beiden Congruenzen

$$\mathfrak{F}(X) \equiv 0\;,\; \mathfrak{F}_1(X) \equiv 0 \; [mod.\; p,\; F(x)]$$

an. Wenn nun eine dieser Congruenzen weniger Wurzeln hätte, als ihr Grad Einheiten enthält, so müsste die andere mehr Wurzeln zulassen, als in ihrem Grade Einheiten enthalten sind; dies ist unmöglich, unser Satz also bewiesen.

367. Lehrsatz II. — Wenn $\Phi(X)$ ein Polynom m^{ten} Grades ist, dessen Coefficienten ganze Zahlen sind, und in welchem der Coefficient von X^m sich nach dem Modul p nicht auf Null reducirt, so kann man eine nach demselben Modul p irreductibele Function $F(x)$ von der Beschaffenheit ermitteln, dass die Congruenz

$$\Phi(X) \equiv 0 \ [mod.\ p,\ F(x)]$$

m Wurzeln besitzt.

Wir zerlegen das Polynom $\Phi(X)$ in Factoren, die nach dem Modul p irreductibel sind; es ergebe sich

$$\Phi(X) \equiv \Phi_1(X)\, \Phi_2(X)\, \Phi_3(X) \ldots (mod.\ p),$$

und die irreductibelen Polynome Φ_1, Φ_2, ... seien beziehungsweise von den Graden n_1, n_2, ... Jeder der angegebenen Factoren von Φ geht nach dem Modul p in eine der Functionen

$$X^{p^{n_1}} - X,\ X^{p^{n_2}} - X,\ X^{p^{n_3}} - X, \ldots$$

auf; bezeichnet also ν die kleinste Zahl, welche gleichzeitig durch n_1, n_2, ... theilbar ist, so sind diese Factoren sämmtlich in

$$X^{p^\nu} - X$$

enthalten. Nimmt man folglich eine irreductibele Function ν^{ten} Grades $F(x)$, so besitzt jede der Congruenzen

$$\left.\begin{array}{l} \Phi_1(X) \equiv 0 \\ \Phi_2(X) \equiv 0 \\ \Phi_3(X) \equiv 0 \\ \ldots\ldots\ldots \end{array}\right\} [mod.\ p,\ F(x)]$$

nach No. 366 so viele Wurzeln, als ihr Grad Einheiten enthält, und daher hat auch die vorgelegte Congruenz so viele gleiche oder ungleiche Wurzeln, als ihr Grad Einheiten enthält.

Eigenschaften der Wurzeln einer Congruenz, in welcher das erste Glied eine irreductibele Function ist, deren Grad gleich dem Grade der Modularfunction oder gleich einem Divisor dieses Grades ist.

368. Lehrsatz. — Es seien $F(x)$ und $\mathfrak{F}(x)$ zwei nach dem Modul p irreductibele ganze Functionen; $F(x)$ habe

den Grad ν, $\mathfrak{F}(x)$ den Grad μ, welche Zahl gleich ν oder gleich einem Divisor von ν ist; bezeichnet dann X_1 irgend eine Wurzel von

$$(1).\qquad \mathfrak{F}(X) \equiv 0 \ [mod.\ p\,,\ F(x)]\,,$$

so sind die Wurzeln dieser Congruenz die kleinsten Reste der Potenzen

$$(2).\qquad X_1\ ,\ X_1^p\ ,\ X_1^{p^2}\ ,\ \ldots\ ,\ X_1^{p^{\mu-1}}\,.$$

Nach No. 347 ist nämlich

$$\mathfrak{F}(X_1^{p^m}) \equiv [F(X_1)]^{p^m} \ (mod.\ p)\,,$$

und da X_1 der Congruenz (1) genügt, so hat man

$$\mathfrak{F}(X_1^{p^m}) \equiv 0 \ [mod.\ p,\ F(x)]\,;$$

folglich ist jede der Potenzen (2) oder ihr kleinster Rest eine Wurzel der vorgelegten Congruenz. Wir haben jetzt noch zu beweisen, dass die Reste dieser Potenzen von einander verschieden sind. Hätte man

$$X_1^{p^{n+n'}} \equiv X_1^{p^{n'}} \ [mod.\ p,\ F(x)]\,,$$

also

$$X_1^{p^{n'}}\left[X_1^{p^{n'}(p^n-1)} - 1\right] \equiv 0 \ [mod.\ p,\ F(x)]\,,$$

so müsste

$$X_1^{p^{n'}(p^n-1)} - 1 \equiv 0 \ [mod.\ p,\ F(x)]$$

sein. Der Exponent, zu welchem X_1 gehört, wäre danach ein Divisor von $p^{n'}(p^n - 1)$, und da derselbe den Factor p nicht enthält, ein Divisor von $p^n - 1$; man hätte folglich

$$X^{p^n} - 1 \equiv 0 \ [mod.\ p,\ F(x)].$$

Dies ist aber unmöglich, da $n < \mu$ ist; mithin sind die Reste der Potenzen (2) von einander verschieden.

Zusatz. — Bezeichnet $F(x)$ eine nach dem Primzahlmodul p irreductibele Function ν^{ten} Grades, so sind die Wurzeln der Congruenz

$$F(X) \equiv 0 \ [mod.\ p,\ F(x)]$$

die kleinsten Reste der ν Potenzen

$$x\ ,\ x^p\ ,\ x^{p^2}\ ,\ \ldots\ ,\ x^{p^{\nu-1}}\,.$$

Primitive Wurzeln der Congruenz

$$X^{p^\nu-1}-1 \equiv 0\ [mod.\ p,\ F(x)].$$

369. Wenn $F(x)$ irgend eine nach dem Primzahlmodul p irreductibele ganze Function ν^{ten} Grades ist, so giebt es nach No. 363 unter den $p^\nu - 1$ Wurzeln der Congruenz

(1). $$X^{p^\nu-1}-1 \equiv 0\ [mod.\ p,\ F(x)]$$

immer $\varphi(p^\nu - 1)$, die zum Exponenten $p^\nu - 1$ gehören; wir nennen dieselben primitive Wurzeln.

Bezeichnet X eine beliebige der primitiven Wurzeln von (1), so sind die Wurzeln dieser Congruenz die kleinsten Reste der Potenzen

$$X\ ,\ X^2\ ,\ X^3,\ \ldots,\ X^{p^\nu-1}.$$

Hat man die Zahl $p^\nu-1$ in ihre Primfactoren zerlegt,

$$p^\nu - 1 = 2^\varrho\ q^\mu\ r^\lambda\ \ldots,$$

so genügt es (No. 364, Zusatz II) zur Ermittlung einer primitiven Wurzel von (1), die Congruenzen

(2). $$X^{2^\varrho} \equiv 1\ ,\ X^{q^\mu} \equiv 1\ ,\ X^{r^\lambda} \equiv 1\ ,\ \ldots\ [mod.\ p,\ F(x)]$$

zu bilden, und solche Wurzeln dieser Congruenzen zu suchen, welche beziehungsweise zu den Exponenten 2^ϱ, q^μ, r^λ, ... gehören. Diese Wurzeln kann man primitive Wurzeln derjenigen der Congruenzen (2) nennen, auf welche sie sich beziehen.

Wenn die Modularfunction $F(x)$ eine der irreductibelen Functionen ν^{ten} Grades ist, welche zum Exponenten $p^\nu - 1$ gehören, so sind die $p^\nu - 1$ Wurzeln der Congruenz (1) offenbar die Reste der Potenzen

$$x\ ,\ x^2\ ,\ x^3\ ,\ \ldots\ ,\ x^{p^\nu-2},\ x^{p^\nu-1};$$

denn in diesem Falle ist x eine primitive Wurzel der Congruenz.

370. Kennt man eine nach dem Modul p irreductibele Function ν^{ten} Grades $F(x)$, und hat mittels dieser Function eine primitive Wurzel der Congruenz

(1). $$X^{p^\nu-1} - 1 \equiv 0\ [mod.\ p,\ F(x)]$$

bestimmt, so kann man leicht alle irreductibeln Functionen ermitteln, deren Grad gleich ν oder gleich einem Divisor von ν ist, mit andern Worten: man kann die Function

$$x^{p^\nu} - x \text{ oder } X^{p^\nu} - X$$

in Factoren zerlegen, welche nach dem Modul p irreductibel sind.

Es sei nämlich X_1 eine primitive Wurzel der Congruenz (1); jede Potenz X_1^e ist Wurzel einer Congruenz

$$(2). \qquad \mathfrak{F}(X) \equiv 0 \; [mod.\; p,\; F(x)],$$

in welcher $\mathfrak{F}(X)$ eine nach dem Modul p irreductibele Function bedeutet, deren Grad μ gleich ν oder gleich einem Divisor von ν ist. Die Wurzeln der Congruenz (2) sind dann (No. 368)

$$(3). \qquad X_1^e,\; X_1^{ep},\; X_1^{ep^2},\; \ldots,\; X_1^{ep^{\mu-1}},$$

und da

$$(4). \qquad X_1^{ep^\mu} \equiv X_1^e \text{ oder } X_1^{e(p^\mu-1)} \equiv 1 \; [mod.\; p,\; F(x)]$$

sein muss, so ist der Exponent $e(p^\mu - 1)$ ein Vielfaches von $p^\nu - 1$. Wir setzen

$$p^\nu - 1 = mn,$$

und nehmen an, m sei der grösste gemeinschaftliche Divisor der Zahlen e und $p^\nu - 1$; dann reducirt sich die Bedingung, unter welcher die Congruenz (4) stattfindet, darauf, dass $p^\mu - 1$ durch n theilbar sei. Damit aber die Functionen (3) wirklich verschieden seien, muss ferner μ die kleinste Zahl sein, für welche n in $p^\mu - 1$ aufgeht.

Hat man auf diese Weise den Grad μ der Congruenz (2) bestimmt, so ist (No. 345) identisch

$$\mathfrak{F}(X) \equiv (X - X_1^e)(X - X_1^{ep}) \ldots (X - X^{ep^{\mu-1}}) \; [mod.\; p,\; F(x)],$$

und durch Ausführung der im zweiten Gliede dieser Formel geforderten Multiplicationen erhält man einen Ausdruck von $\mathfrak{F}(X)$, in welchem die Veränderliche x nicht mehr vorkommt.

So kann man alle irreductibelen Functionen bilden, in welche sich die Function $X^{p^\nu} - X$ zerlegen lässt.

Bezeichnet k den Exponenten, zu welchem X_1^e gehört, so ist

$$X_1^{ke} \equiv 1 \; [mod.\; p,\; F(x)];$$

daraus ergiebt sich, dass ke durch $p^\nu - 1 = mn$ theilbar, dass also k ein Vielfaches von n ist. Nun wird aber die vorhergehende Congruenz befriedigt, wenn man $k = n$ annimmt; folglich gehört X^e zum Exponenten n.

Wir behaupten ausserdem, dass die irreductibele Function $\mathfrak{F}(X)$ zum Exponenten n gehöre. Bezeichnen nämlich $\mathfrak{F}_1(X)$ und $\Phi(X)$ den Quotienten und den Rest der in Beziehung auf den Modul p vollzogenen Division von $X^n - 1$ durch $\mathfrak{F}(X)$, so hat man

$$X^n - 1 = \mathfrak{F}(X)\,\mathfrak{F}_1(X) + \Phi(X) + p\,\chi(X),$$

wo χ eine ganze Function bedeutet. Dies vorausgesetzt, lassen die Congruenzen

$$X^n - 1 \equiv 0\ ,\ \mathfrak{F}(X) \equiv 0\ [mod.\ p,\ F(x)]$$

die μ Wurzeln zu, welche die Reihe (3) bilden; diese μ Wurzeln gehören daher auch der Congruenz

$$\Phi(X) \equiv 0\ [mod.\ p,\ F(x)]$$

an. Da nun der Grad von Φ nicht grösser als $\mu - 1$ sein kann, so besteht die letzte Congruenz nothwendig identisch, und man hat

$$\Phi(X) \equiv 0\ (mod.\ p),$$

folglich

$$X^n - 1 = \mathfrak{F}(X)\,\mathfrak{F}_1(X) + p\,\chi(X);$$

diese Formel ist der Ausdruck des angegebenen Satzes.

371. Aus der vorstehenden Betrachtung entnehmen wir Folgendes:

Will man alle irreductibelen Functionen ν^{ten} Grades bilden, die zum Exponenten n gehören, welche Zahl n ein $p^\nu - 1$ eigener Divisor ist, so setze man

$$p^\nu - 1 = mn,$$

und lasse e irgend eins der Vielfachen von m bedeuten, die prim zu n sind. Dann ist der allgemeine Ausdruck der gesuchten Functionen

$$\mathfrak{F}(X) \equiv (X - X_1^e)\,(X - X_1^{ep}) \ldots (X - X_1^{ep^{\nu-1}})\ [mod.\ p,\ F(x)].$$

Will man die irreductibelen Functionen erhalten, die zum Exponenten $p^\nu - 1$ gehören, und denen die primitiven Wurzeln entsprechen, so mache man $m = 1$, $n = p^\nu - 1$, so dass es genügt, in der vorhergehenden Formel für e alle Zahlen zu nehmen, die prim zu $p^\nu - 1$ und zu p sind.

Ueber den Gesichtspunkt, aus welchem Galois die nach einem Primzahlmodul und einer Modularfunction genommenen Congruenzen betrachtet hat.

372. In der Theorie der gewöhnlichen Congruenzen sieht man jede durch den Modul theilbare Zahl als Null an. Ebenso verfährt man in der Untersuchung der Congruenzen von der Form

$$\mathfrak{F}(X, x) \equiv 0 \; [mod.\; p, F(x)],$$

als verschwänden die Vielfachen von $F(x)$. Nun giebt es hier eine unbestimmte Grösse x, deren man sich naturgemäss dazu bedienen kann, die Vielfachen von $F(x)$ zum Verschwinden zu bringen; es genügt in der That, die Uebereinkunft zu treffen, dass diese unbestimmte Grösse x eine imaginäre Wurzel der irreductibelen Congruenz

$$F(x) \equiv 0 \; (mod.\; p)$$

sei. Auf diese Weise können in die Analysis neue imaginäre Grössen eingeführt werden, deren Anwendung zwar nicht unumgänglich nöthig, aber mit gewissen Vortheilen verbunden ist. Diese Auffassung rührt von Galois her, der sie eingehend im Bulletin des Sciences mathématiques de Férussac (t. XIII, p. 398) dargelegt hat. Der von Galois 1830 veröffentlichte Artikel ist mit dessen übrigen Arbeiten nochmals abgedruckt im Journal de Mathématiques pures et appliquées t. XI.

Die in den vorhergehenden Nummern entwickelte Theorie liefert uns von Galois' Gesichtspunkte aus folgende Sätze:

Lehrsatz I. — Bezeichnet i eine imaginäre Wurzel der irreductibelen Congruenz ν^{ten} Grades

$$F(x) \equiv 0 \; (mod.\; p),$$

so kann eine nicht identische Congruenz m^{ten} Grades

$$\varphi(x) \equiv 0 \; (mod.\; p)$$

nicht mehr als m verschiedene Wurzeln von der Form

$$a_0 + a_1 i + a_2 i^2 + \cdots + a_{\nu-1} i^{\nu-1}$$

haben, wo $a_0, a_1, \ldots, a_{\nu-1}$ ganze Zahlen bezeichnen, die kleiner als p sind.

Lehrsatz II. — Die Congruenz

$$x^{p^\nu} - x \equiv 0 \; (mod.\; p)$$

lässt alle p^ν Wurzeln von der Form

$$a_0 + a_1 i + a_2 i^2 + \cdots + a_{\nu-1} i^{\nu-1}$$

zu, in welcher i eine Wurzel der irreductibelen Congruenz ν^{ten} Grades

$$F(x) \equiv 0 \ (mod.\ p)$$

bezeichnet.

Lehrsatz III. — Die irreductibele Congruenz ν^{ten} Grades

$$F(x) \equiv 0 \ (mod.\ p)$$

lässt ν Wurzeln zu, die durch

$$i\,,\ i^p\,,\ i^{p^2}\,,\ \ldots,\ i^{p^{\nu-1}}$$

dargestellt werden können.

Lehrsatz IV. — Jede nicht identische Congruenz hat so viele gleiche oder ungleiche Wurzeln, als ihr Grad Einheiten enthält; alle diese Wurzeln sind ganze Functionen ein und derselben imaginären Wurzel einer irreductibelen Congruenz.

Lehrsatz V. — Die Congruenz

$$x^{p^\nu-1} - 1 \equiv 0 \ (mod.\ p)$$

besitzt primitive Wurzeln; jede derselben ist Wurzel einer irreductibelen Congruenz ν^{ten} Grades, und ihre Potenzen liefern alle Wurzeln der vorgelegten Congruenz.

Lehrsatz VI. — Hat man

$$p^\nu - 1 = q_1^{\alpha_1}\ q_2^{\alpha_2} \cdots q_m^{\alpha_m}\,,$$

wo $q_1, q_2, \ldots, q_m$ ungleiche Primzahlen und $\alpha_1, \alpha_2, \ldots, \alpha_m$ irgend welche ganze Zahlen sind, und bezeichnen

$$r_1\,,\ r_2\,,\ \ldots\,,\ r_m$$

beziehungsweise primitive Wurzeln der Congruenzen

$$x^{q_1^{\alpha_1}} - 1 \equiv 0\,,\ x^{q_2^{\alpha_2}} - 1 \equiv 0\,,\ \ldots,\ x^{q_m^{\alpha_m}} - 1 \equiv 0 \ (mod.\ p)\,,$$

so ist das Produkt $r_1\, r_2 \ldots r_m$ eine primitive Wurzel der Congruenz

$$x^{p^\nu-1} - 1 \equiv 0 \ (mod.\ p).$$

Anwendung der vorhergehenden Theorie auf den Fall des Moduls 7.

373. Es wird von Nutzen sein, einige Fälle eines bestimmten Moduls zu untersuchen. Zu diesem Zwecke wählen wir den Modul 7, für welchen 3 eine primitive Wurzel ist; die Reste in Beziehung auf diesen Modul nehmen wir zwischen den Grenzen -3 und $+3$ an.

Die Congruenz $x^{7^2-1}-1\equiv 0$ (*mod.* 7). — Der Lehrsatz der No. 358 liefert uns unmittelbar die drei irreductibelen Functionen zweiten Grades

$$x^2+1\,,\;x^2+2\,,\;x^2-3.$$

Wir stellen uns jetzt auf den Standpunkt von Galois und wollen eine primitive Wurzel der Congruenz

(1). $$x^{7^2-1}-1\equiv 0 \text{ oder } x^{48}-1\equiv 0$$

ermitteln, indem wir von der Wurzel i der irreductibelen Congruenz

(2). $$x^2+1\equiv 0\ (mod.\ 7)$$

ausgehen. Da $48=2^4\times 3$ ist, so müssen wir eine primitive Wurzel der beiden Congruenzen

(3). $$x^3-1\equiv 0\,,\;x^{16}-1\equiv 0\ (mod.\ 7)$$

kennen lernen. Die erste dieser Congruenzen hat die primitive Wurzel 2, und die primitiven Wurzeln der zweiten gehören der Congruenz

(4). $$x^8+1\equiv 0\ (mod.\ 7)$$

an, welche, weil $i^2\equiv -1$ ist, in die beiden folgenden zerfällt:

$$x^4-i\equiv 0\,,\;x^4+i\equiv 0\ (mod.\ 7).$$

Betrachten wir die erste dieser Congruenzen

$$x^4-i\equiv 0\ (mod.\ 7)$$

und setzen

$$x=a_0+a_1 i,$$

so ergiebt sich

$$a_0^4-3a_0^3a_1 i-a_0^2a_1^2i^2-3a_0a_1^3i^3+a_1^4i^4\equiv i\ (mod.\ 7),$$

oder, wenn wir mittels der Relation $i^2\equiv -1$ reduciren,

$$(a_0^4+a_0^2a_1^2+a_1^4)+(-3a_0^3a_1+3a_0a_1^3-1)\,i\equiv 0\ (mod.\ 7),$$

folglich

$$a_0^4+a_0^2a_1^2+a_1^4\equiv 0\,,\;-3a_0^3a_1+3a_0a_1^3-1\equiv 0\ (mod.\ 7).$$

Man genügt diesen Congruenzen dadurch, dass man

$$a_0 = 2 \ , \ a_1 = -3$$

setzt; die zweite der Congruenzen (3) hat daher die primitive Wurzel $2-3i$, und mithin ist

$$(5). \qquad x = 2 \times (2-3i) \equiv -3 + i \ (mod.\ 7)$$

primitive Wurzel der vorgelegten Congruenz. Aus (5) folgt

$$(6). \qquad x^2 \equiv 2 + i + i^2 \equiv 1 + i,$$

und wenn i aus (5) und (6) eliminirt wird,

$$x^2 - x + 3 \equiv 0 \ (mod.\ 7).$$

Dies ist die irreductibele Congruenz, von welcher die gesuchte primitive Wurzel abhängt. Stellt man diese Wurzel durch i dar, so sind die 48 Wurzeln der Congruenz (1) die mittels der Congruenz

$$i^2 - i + 3 \equiv 0 \ (mod.\ 7)$$

reducirten Werthe der Potenzen

$$i \ , \ i^2 \ , \ i^3 \ , \ \ldots \ , \ i^{48}.$$

374. Die Congruenz $x^{7^3-1} - 1 \equiv 0 \ (mod.\ 7)$. — Der Satz der No. 358 zeigt für den Modul 7 die Existenz der vier irreductibelen Functionen dritten Grades

$$x^3 - 2 \ , \ x^3 - 3 \ , \ x^3 + 3 \ , \ x^3 + 2$$

an. Bezeichnet i eine Wurzel der Congruenz

$$i^3 \equiv 2 \ (mod.\ 7),$$

so sind die Wurzeln der vorgelegten Congruenz von der Form

$$a_0 + a_1 i + a_2 i^2.$$

Wir wollen nun eine primitive Wurzel der vorgelegten Congruenz

$$(1). \qquad x^{342} - 1 \equiv 0 \text{ oder } x^{2 \cdot 3^2 \cdot 19} - 1 \equiv 0 \ (mod.\ 7)$$

ermitteln. Zu diesem Zwecke genügt es, eine primitive Wurzel jeder der drei folgenden Congruenzen zu erhalten:

$$(2). \qquad x^2 - 1 \equiv 0 \ , \ x^{3^2} - 1 \equiv 0 \ , \ x^{19} - 1 \equiv 0 \ (mod.\ 7).$$

Die primitive Wurzel der ersten der Congruenzen (2) ist -1. Die zweite der Congruenzen (2) kann auf die Form

$$(x^3 - 1)(x^3 - 2)(x^3 + 3) \equiv 0 \ (mod.\ 7)$$

gebracht werden, und ihre primitiven Wurzeln sind die Wurzeln der beiden Congruenzen

$$x^3 \equiv 2 \; , \; x^3 \equiv -3 \; (mod.\; 7);$$

folglich ist i primitive Wurzel der zweiten der Congruenzen (2).

Es ist jetzt noch eine Wurzel von $x^{19} - 1 \equiv 0$, oder vielmehr von

$$\frac{x^{19}-1}{x-1} \equiv 0 \; (mod.\; 7)$$

zu suchen. Sehen wir, ob man dieser Congruenz genügen kann, wenn man einfach $x = a_0 + a_1 i$ statt $a_0 + a_1 i + a_2 i^2$ setzt. Wir müssen

$$(a_0 + a_1 i)^{19} \equiv 1 \; (mod.\; 7)$$

haben; wird das erste Glied dieser Congruenz nach dem binomischen Satze entwickelt, und werden die Potenzen von a_0, a_1 und i mittels der Formeln

$$a_0^{6m} \equiv 1 \; , \; a_1^{6m} \equiv 1 \; , \; i^3 \equiv 2 \; (mod.\; 7)$$

reducirt, so geht dieselbe über in

$$3\,[a_0 - a_0^4\, a_1^3 + (a_0^5\, a_1^2 + a_0^2\, a_1^5)\; i^2] \equiv 1;$$

es muss also

$$3\, a_0 - 3\, a_0^4\, a_1^3 \equiv 1 \; , \; a_0^5\, a_1^2 + a_0^2\, a_1^5 \equiv 0$$

sein. Diese beiden letzten Bedingungen werden durch die Werthe

$$a_0 = -1 \; , \; a_1 = +1$$

erfüllt; folglich ist $-1 + i$ eine primitive Wurzel der dritten der Congruenzen (2). Das Produkt der drei Grössen

$$-1 \; , \; i \; , \; -1 + i,$$

welches gleich

$$i - i^2$$

ist, muss daher eine primitive Wurzel der vorgelegten Congruenz

$$x^{7^3-1} - 1 \equiv 0 \; (mod.\; 7)$$

sein, und mithin besitzt dieser Ausdruck die Eigenschaft, dass seine Potenzen $7^3 - 1$ verschiedene Ausdrücke von der Form

$$a_0 + a_1 i + a_2 i^2$$

liefern.

Will man die irreductibele Congruenz kennen lernen, von welcher die eben gefundene Wurzel abhängt, so hat man i aus

$$x = i - i^2 \text{ und } i^3 \equiv 2 \; (mod.\; 7)$$

zu eliminiren. Wird der Werth von x auf die dritte Potenz erhoben, so ergiebt sich nach Reduction der Exponenten von i

$$x^3 \equiv -2 + i - i^2 \ (mod.\ 7),$$

folglich ist

$$x^3 - x + 2 \equiv 0 \ (mod.\ 7).$$

Es ist zweckmässig, die Wurzel dieser Congruenz, die durch i dargestellt werden möge, als **Basis** der imaginären Grössen anzusehen, so dass also

$$i^3 - i + 2 \equiv 0 \ (mod.\ 7)$$

ist; dann erhält man alle imaginären Grössen von der Form

$$a_0 + a_1 i + a_2 i^2$$

dadurch, dass man i auf alle Potenzen erhebt, und mittels der vorhergehenden Congruenz reducirt.

375. Die Congruenz $x^{7^4-1} - 1 \equiv 0 \ (mod.\ 7)$. — Der Satz der No. 354 lehrt uns eine nach dem Modul 7 irreductibele Function vierten Grades kennen, nämlich

$$\frac{x^5-1}{x-1} \text{ oder } x^4 + x^3 + x^2 + x + 1;$$

in der That ist der Modul 7 primitive Wurzel für die Primzahl 5. Ausserdem lässt sich jede der drei binomischen Functionen

$$x^{16} + 1 \ , \ x^{16} + 2 \ , \ x^{16} - 3$$

dem in No. 358 bewiesenen Satze zufolge in vier Factoren vierten Grades zerlegen, welche nach dem Modul 7 irreductibel sind. Die Entwicklung der No. 359 lehrt, dass diese Factoren beziehungsweise folgende sind:

$$\begin{array}{lll}
x^4 + x^2 - 1\ , & x^4 + 2x^2 - 2\ , & x^4 + x^2 + 3\ , \\
x^4 - x^2 - 1\ , & x^4 - 2x^2 - 2\ , & x^4 - x^2 + 3\ , \\
x^4 + 3x^2 - 1\ , & x^4 + 3x^2 - 2\ , & x^4 + 2x^2 + 3\ , \\
x^4 - 3x^2 - 1\ , & x^4 - 3x^2 - 2\ , & x^4 - 2x^2 + 3\ .
\end{array}$$

Wir bezeichnen mit i eine Wurzel der Congruenz

$$(1). \qquad i^4 + 3i^2 - 2 \equiv 0 \ (mod.\ 7),$$

und suchen eine primitive Wurzel der Congruenz

$$(2). \qquad x^{7^4-1} - 1 \equiv 0 \text{ oder } x^{2400} - 1 \equiv 0 \ (mod.\ 7).$$

Da $2400 = 2^5 \cdot 3 \cdot 5^2 = 32 \times 3 \times 25$ ist, so müssen wir eine primitive Wurzel jeder der drei Congruenzen

(3). $x^{32}-1\equiv 0\ ,\ x^3-1\equiv 0\ ,\ x^{25}-1\equiv 0\ (mod.\ 7)$
kennen lernen.

Nun liefert die Congruenz (1)

$$(4).\qquad \left.\begin{cases} i^4\equiv 2-3i^2\\ i^8\equiv 1+3i^2\\ i^{16}\equiv -2\end{cases}\right\}\ (mod.\ 7),$$

folglich hat man

$$(i^{16})^3=(i^3)^{16}\equiv -1\ (mod.\ 7).$$

Daraus geht hervor, dass i^3 eine primitive Wurzel der ersten der Congruenzen (3) ist. Die zweite Congruenz (3) lässt 2 als primitive Wurzel zu. Es ist somit nur noch für die dritte Congruenz (3) eine primitive Wurzel aufzufinden; wir wollen versuchen, ob derselben durch

$$x=ai+bi^2$$

genügt werden kann. Wird dieser Werth in

$$x^{25}\equiv 1\ (mod.\ 7)$$

eingesetzt, so ergiebt sich, wenn man mittels der Formeln (4) reducirt und sodann die Coefficienten der Potenzen von i der Null congruent setzt,

$$\left.\begin{aligned} -2a^4b+3a^2b^3-b^5&\equiv 0\\ 2a^5+3a^3b^2-2ab^4&\equiv 0\\ -a^4b+2a^2b^3-b^5+1&\equiv 0\\ -3a^5-2a^3b^2+ab^4+1&\equiv 0\end{aligned}\right\}\ (mod.\ 7).$$

Diese Congruenzen werden durch die Werthe $a=3$, $b=2$ befriedigt. Da man sich nun leicht überzeugen kann, dass $3i+2i^2$ der Congruenz $x^5-1\equiv 0$ nicht genügt, so ist dieser Ausdruck eine primitive Wurzel von $x^{25}-1\equiv 0$. Die vorgelegte Congruenz besitzt daher die primitive Wurzel

$$x=2i^3(3i+2i^2)=-i^4-3i^5,$$

oder, mit Rücksicht auf (4),

$$(5).\qquad x=-2+i+3i^2+2i^3.$$

Daraus folgt

$$(6).\qquad \begin{cases} x^2=-1-i+i^2-3i^3\\ x^3=-1+i-3i^2+2i^3\\ x^4=3-3i+i^3,\end{cases}$$

und durch Elimination von i erhält man

(7). $$x^4 - 2x^3 - 2x - 2 \equiv 0 \ (mod.\ 7).$$

Bezeichnen wir jetzt mit i eine Wurzel der Congruenz (7), so liefern die 2400 ersten Potenzen von i alle Wurzeln der Congruenz

$$x^{2400} - 1 \equiv 0 \ (mod.\ 7).$$

376. Was die nach dem Modul 7 irreductibelen Functionen betrifft, deren Grad grösser als 4 ist, so beschränken wir uns auf einige Andeutungen, die der Leser ohne sonderliche Schwierigkeit wird weiter entwickeln können. Wir haben keinen Lehrsatz, der es gestattet, eine nach dem Modul 7 irreductibele Function 5ten Grades direkt zu bilden. Man kann eine solche aber leicht auf dem Wege des Versuchs ermitteln. So erkennt man, dass die Function

$$x^5 + x - 3$$

nach dem Modul 7 irreductibel ist. Fände nämlich das Gegentheil statt, so würde diese Function einen Divisor ersten oder zweiten Grades besitzen, welcher zugleich der Function $x^{48} - 1$ angehören würde. Man überzeugt sich aber leicht, dass die letzte Function mit der vorgelegten keinen Divisor in Beziehung auf den Modul 7 gemeinschaftlich hat. Die Function $x^5 + x - 3$ gehört zum Exponenten $7^5 - 1$, so dass, wenn i eine Wurzel der irreductibelen Congruenz

$$i^5 + i - 3 \equiv 0 \ (mod.\ 7)$$

bezeichnet, die $7^5 - 1$ ersten Potenzen von i die Wurzeln von

$$x^{7^5-1} - 1 \equiv 0 \ (mod.\ 7)$$

liefern.

Es giebt zwei irreductibele binomische Functionen 6ten Grades, nämlich $x^6 + 2$ und $x^6 - 3$, und aus jeder derselben lässt sich leicht eine primitive Wurzel der Congruenz

$$x^{7^6-1} - 1 \equiv 0 \ (mod.\ 7)$$

herleiten. Setzt man z. B.

$$i^6 \equiv -2 \ (mod.\ 7),$$

so genügt es, für jede der vier Congruenzen

$$x^{16} - 1 \equiv 0,\ x^9 - 1 \equiv 0,\ x^{19} - 1 \equiv 0,\ x^{43} - 1 \equiv 0 \ (mod.\ 7)$$

eine primitive Wurzel zu bestimmen; dabei verfahren wir, wie in den oben erörterten Fällen. Man erkennt leicht, dass $1 + i$

eine primitive Wurzel der vorgelegten Congruenz ist. Diese Wurzel gehört der folgenden irreductibelen Congruenz an:

$$(x-1)^6+2\equiv 0 \ (mod.\ 7).$$

Was endlich den 7ten Grad betrifft, so lehrt uns der Satz der No. 360 eine irreductibele Function, nämlich x^7-x-g kennen, worin g von Null verschieden ist. Bezeichnet i eine Wurzel der irreductibelen Congruenz

$$i^7-i-3\equiv 0 \ (mod.\ 7),$$

so ist i primitive Wurzel für die Congruenz

$$x^{7^7-1}-1\equiv 0 \ (mod.\ 7).$$

Viertes Kapitel.

Ueber die Anzahl der zwischen gegebenen Grenzen enthaltenen Primzahlen.

Näherungsweise Berechnung des Produkts 1 . 2 . 3 ... x, wenn x eine grosse Zahl ist.

377. Die Theorie, die ich in diesem Kapitel besonders im Auge habe, fordert, dass man die ersten Terme der Reihe kenne, durch welche der Logarithmus des Produkts der x ersten ganzen Zahlen ausgedrückt wird. Diese berühmte Reihe rührt von Stirling her und war der Gegenstand der Untersuchungen vieler Mathematiker, von welchen namentlich Cauchy, Binet, Malmsten und Liouville zu erwähnen sind. Ich glaube aber nicht, dass es unter den verschiedenen Beweisen, die man für diese Formel besitzt, einen giebt, der einfacher als derjenige wäre, den ich am 2. April 1860 der Akademie der Wissenschaften vorgelegt und in einer Note zur 6. Auflage von Lacroix, traité élémentaire de Calcul différentiel et intégral nochmals mitgetheilt habe. In dieser Note habe ich gezeigt, dass die bekannte Formel von Wallis völlig zur Begründung der Stirling'schen Formel ausreicht; dazu ist die Herleitung so leicht, dass man die zweite Formel gewissermassen als eine Umänderung der ersteren ansehen kann. Ich werde hier nicht alle Entwicklungen, die ich a. a. O. über diesen Gegenstand angestellt habe, wiederholen, sondern mich auf die Begründung derjenigen Resultate beschränken, welche für die hier zu erörternden Fragen unentbehrlich sind.

Wir erinnern zunächst daran, dass die Formel von Wallis, von der wir ausgehen, aus der bekannten Formel

$$\cos z = \left(1 - \frac{4z^2}{\pi^2}\right)\left(1 - \frac{4z^2}{9\pi^2}\right)\left(1 - \frac{4z^2}{25\pi^2}\right)\cdots$$

hergeleitet werden kann, mittels welcher die Function $\cos z$ als Produkt unendlich vieler linearer Factoren dargestellt wird. Letztere Formel kann in folgender Weise geschrieben werden:

$$\frac{\pi}{2} \frac{\sin\left(\frac{\pi}{2} - z\right)}{\frac{\pi}{2} - z} = \left(1 + \frac{2z}{\pi}\right)\left(1 - \frac{4z^2}{9\pi^2}\right)\left(1 - \frac{4z^2}{25\pi^2}\right) \cdots,$$

und wenn man $z = \frac{\pi}{2}$ macht, so folgt

$$\frac{\pi}{2} = 2\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{25}\right)\left(1 - \frac{1}{49}\right) \cdots \left(1 - \frac{1}{(2x-1)^2}\right) \text{ (für } x = \infty),$$

oder

$$\frac{\pi}{2} = \frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdots \frac{2x-2}{2x-3} \cdot \frac{2x-2}{2x-1} \cdot \frac{2x}{2x-1} \text{ (für } x = \infty),$$

und dies ist die Formel von Wallis.

378. Diese Formel nimmt die sehr einfache Form

$$\frac{[\varphi(x)]^4}{[\varphi(2x)]^2} = 1 \text{ (für } x = \infty),$$

oder

$$(1). \qquad \frac{[\varphi(x)]^2}{\varphi(2x)} = 1 \text{ (für } x = \infty)$$

an, wenn

$$(2). \qquad \varphi(x) = \frac{1 \cdot 2 \cdot 3 \cdots x}{\sqrt{2\pi} \cdot e^{-x} \cdot x^{x+\frac{1}{2}}}$$

gesetzt wird; e bezeichnet die Basis der natürlichen Logarithmen.

Aus (2) folgt

$$(3). \qquad \frac{\varphi(x)}{\varphi(x+1)} = \frac{1}{e}\left(1 + \frac{1}{x}\right)^{x+\frac{1}{2}} = e^{-1+\left(x+\frac{1}{2}\right)\log\left(1+\frac{1}{x}\right)},$$

oder

$$(4). \qquad \log\frac{\varphi(x)}{\varphi(x+1)} = -1 + \left(x + \frac{1}{2}\right)\log\left(1 + \frac{1}{x}\right);$$

in diesen und den folgenden Formeln ist überall von natürlichen Logarithmen die Rede. Nun ist für $x > 1$

$$\log\left(1 + \frac{1}{x}\right) = \frac{1}{x} - \frac{1}{2x^2} + \frac{1}{3x^3} - \cdots + \frac{(-1)^{n-1}}{nx^n} + \cdots,$$

also

$$\left(x + \frac{1}{2}\right)\log\left(1 + \frac{1}{x}\right) = 1 + \frac{1}{12x^2} - \frac{1}{12x^3} + \cdots + \frac{n-1}{2n(n+1)} \cdot \frac{(-1)^n}{x^n} + \cdots,$$

folglich hat man

$$(5). \quad \begin{cases} \log \dfrac{\varphi(x)}{\varphi(x+1)} = \dfrac{1}{12x^2} - \dfrac{1}{12x^3} + \dfrac{3}{40x^4} - \cdots \\ \qquad + \dfrac{(n-1)}{2n(n+1)} \cdot \dfrac{(-1)^n}{x^n} + \cdots . \end{cases}$$

Die Terme dieser Reihe sind abwechselnd positiv und negativ; ausserdem ist der absolute Werth des Verhältnisses des n^{ten} Terms zum vorhergehenden Terme

$$\frac{n^2}{n^2+n-2} \cdot \frac{1}{x}.$$

Für $n = 2$ ist dieses Verhältniss gleich $\frac{1}{x}$; es ist aber kleiner als $\frac{1}{x}$, wenn $n > 2$ ist. Wenn daher auch x sich auf 1 reducirte, so würden doch die absoluten Werthe der Terme der Reihe (5), vom zweiten Terme an, beständig kleiner werden. Daraus geht hervor, dass

$$\log \frac{\varphi(x)}{\varphi(x+1)} < \frac{1}{12x^2},$$

oder

$$(6). \quad \frac{\varphi(x)}{\varphi(x+1)} < e^{\frac{1}{12x^2}}$$

sein muss. Wir wollen aber noch eine kleinere Grenze für

$$\frac{\varphi(x)}{\varphi(x+1)}$$

ermitteln, die uns später von Nutzen sein wird.

Multiplicirt man nämlich die Formel (5) mit $x+1$, so ergiebt sich

$$(x+1) \log \frac{\varphi(x)}{\varphi(x+1)} = \frac{1}{12x} - \frac{1}{120x^3} + \cdots$$
$$+ \frac{(n-3)}{2(n-1)n(n+1)} \cdot \frac{(-1)^{n-1}}{x^{n-1}} + \cdots .$$

Dieser Reihe fehlt der Term in $\frac{1}{x^2}$; die übrigen Terme sind abwechselnd positiv und negativ, und das Verhältniss des Terms in $\frac{1}{x^n}$ zu dem Terme in $\frac{1}{x^{n-1}}$ hat den absoluten Werth

$$\frac{(n-1)(n-2)}{(n-1)(n-2)+2(n-4)} \cdot \frac{1}{x},$$

welcher $= \frac{1}{x}$ oder $< \frac{1}{x}$ ist, je nachdem $n = 4$ oder > 4

ist. Die Terme der letzten Reihe nehmen daher vom zweiten Terme an, auch wenn $x = 1$ ist, beständig ab, und man hat

$$(x+1) \log \frac{\varphi(x)}{\varphi(x+1)} < \frac{1}{12x},$$

oder

$$\log \frac{\varphi(x)}{\varphi(x+1)} < \frac{1}{12x(x+1)}. \tag{7}$$

379. Die Formel (6) zeigt, dass

$$\frac{\varphi(x)}{\varphi(x+1)} = e^{\frac{\vartheta_0}{x^2}} \tag{8}$$

ist, worin ϑ_0 eine zwischen 0 und $\frac{1}{12}$ liegende Zahl bedeutet. Sind $\vartheta_1, \vartheta_2, \ldots, \vartheta_{x-1}$ Zahlen, welche demselben Intervalle angehören, so folgt aus (8), wenn x in

$$x+1, \; x+2, \; \ldots, \; 2x-1$$

verwandelt wird,

$$\left\{\begin{aligned} \frac{\varphi(x+1)}{\varphi(x+2)} &= e^{\frac{\vartheta_1}{(x+1)^2}}, \\ \frac{\varphi(x+2)}{\varphi(x+3)} &= e^{\frac{\vartheta_2}{(x+2)^2}}, \\ &\ldots\ldots\ldots\ldots, \\ \frac{\varphi(2x-1)}{\varphi(2x)} &= e^{\frac{\vartheta_{x-1}}{(2x-1)^2}}. \end{aligned}\right. \tag{9}$$

Wir multipliciren die Formeln (8) und (9) in einander. Da die Summe der x Brüche

$$\frac{\vartheta_0}{x^2} + \frac{\vartheta_1}{(x+1)^2} + \frac{\vartheta_2}{(x+2)^2} + \cdots + \frac{\vartheta_{x-1}}{(2x-1)^2}$$

kleiner als

$$\frac{1}{12} \cdot \frac{1}{x^2} \times x = \frac{1}{12x}$$

ist, so erhält man

$$\frac{\varphi(x)}{\varphi(2x)} = e^{\frac{\vartheta}{x}}; \tag{10}$$

ϑ ist eine positive Zahl und kleiner als $\frac{1}{12}$.

Es ist somit

$$\frac{\varphi(x)}{\varphi(2x)} = 1 \quad (\text{für } x = \infty). \tag{11}$$

Dividirt man jetzt die Formel (1) durch (11), so ergiebt sich

(12) $$\varphi(x) = 1 \text{ (für } x = \infty),$$

d. h., der Formel (2) wegen,

(13). $$1 \cdot 2 \cdot 3 \cdots x = \sqrt{2\pi} \cdot e^{-x} x^{x+\frac{1}{2}} (1 + \varepsilon_x);$$

darin bezeichnet ε_x eine für $x = \infty$ verschwindende Grösse, für welche wir noch eine obere Grenze zu bestimmen haben.

380. Wir setzen, wie wir bereits im II[ten] Theile dieses Werks thaten,

(14). $$\Gamma(x+1) = 1 \cdot 2 \cdot 3 \cdots x.$$

Mittels der vorhergehenden Betrachtung lässt sich leicht ein vollständiger Ausdruck des Produkts $\Gamma(x+1)$ oder, was auf dasselbe hinausläuft, ein Ausdruck des natürlichen Logarithmus $\log \Gamma(x+1)$ ermitteln. Aus Formel (2) folgt zunächst

(15). $$\log \Gamma(x+1) = \tfrac{1}{2} \log 2\pi - x + (x + \tfrac{1}{2}) \log x + \log \varphi(x);$$

ferner besteht die Identität

$$\log \varphi(x) = \log \frac{\varphi(x)}{\varphi(x+1)} + \log \frac{\varphi(x+1)}{\varphi(x+2)} + \cdots$$
$$+ \log \frac{\varphi(x+m)}{\varphi(x+m+1)} + \log \varphi(x+m+1).$$

Wenn aber die ganze Zahl m unbegrenzt wächst, so nähert sich [Formel (12)] $\varphi(x+m+1)$ der Einheit, also $\log \varphi(x+m+1)$ der Null; es ist daher

(16) $$\log \varphi(x) = \sum_{m=0}^{m=\infty} \log \frac{\varphi(x+m)}{\varphi(x+m+1)},$$

oder, der Formel (4) wegen,

(17). $$\log \varphi(x) = \sum_{m=0}^{m=\infty} \left[\left(x + m + \frac{1}{2}\right) \log \left(1 + \frac{1}{x+m}\right) - 1\right];$$

folglich geht (15) über in

(18). $$\begin{cases} \log \Gamma(x+1) = \frac{1}{2} \log 2\pi - x + \left(x + \frac{1}{2}\right) \log x \\ \qquad + \sum_{m=0}^{m=\infty} \left[\left(x + m + \frac{1}{2}\right) \log \left(1 + \frac{1}{x+m}\right) - 1\right]. \end{cases}$$

Diese von Gudermann gefundene Formel (18) lässt sich, wie man sieht, leicht aus der Wallis'schen Formel herleiten.

381. Aus der Formel (18) kann man zu der von Stirling gelangen; wir wollen indess diese Transformation nicht vornehmen, sondern uns darauf beschränken, die uns nöthigen Grenzen von $\log \Gamma(x+1)$ zu bestimmen.

Da die Grösse $\log \varphi(x)$ positiv ist, so liefert die Formel (15)

$$(19). \quad \log \Gamma(x+1) > \tfrac{1}{2} \log 2\pi - x + (x + \tfrac{1}{2}) \log x.$$

Ferner erhalten wir aus Formel (16), bei Berücksichtigung der Ungleichung (7),

$$\log \varphi(x) < \sum_{m=0}^{m=\infty} \frac{1}{12(x+m)(x+m+1)}.$$

Nun ist

$$\frac{1}{(x+m)(x+m+1)} = \frac{1}{x+m} - \frac{1}{x+m+1},$$

folglich

$$12 \log \varphi(x) < \left(\frac{1}{x} - \frac{1}{x+1}\right) + \left(\frac{1}{x+1} - \frac{1}{x+2}\right) + \left(\frac{1}{x+2} - \frac{1}{x+3}\right) + \cdots.$$

Da die Summe der Reihe, welche das zweite Glied dieser Formel bildet, gleich $\frac{1}{x}$ ist, so folgt

$$\log \varphi(x) < \frac{1}{12x},$$

und es ist somit

$$(20). \quad \log \Gamma(x+1) < \frac{1}{2} \log 2\pi - x + \left(x + \frac{1}{2}\right) \log x + \frac{1}{12x}.$$

Die Formeln (19) und (20) enthalten die beiden Grenzen, die wir ermitteln wollten. Gehen wir von den Logarithmen zu den Zahlen über, so ergiebt sich

$$(21). \quad \begin{cases} 1 \cdot 2 \cdot 3 \cdots x > \sqrt{2\pi}\, e^{-x} \cdot x^{x+\frac{1}{2}}, \\ 1 \cdot 2 \cdot 3 \cdots x < \sqrt{2\pi}\, e^{-x+\frac{1}{12x}} \cdot x^{x+\frac{1}{2}}. \end{cases}$$

Ausdehnung der vorhergehenden Formeln auf den Fall, in welchem x nicht mehr eine ganze positive Zahl ist.

382. Man bezeichnet gewöhnlich mit dem Symbol $\Gamma(x+1)$ eine gewisse Function von x, die für alle reellen und complexen

Werthe von x einen bestimmten Werth hat, die nur dann unendlich gross wird, wenn x gleich einer negativen ganzen Zahl ist, und die für ganze positive Werthe von x sich auf das Produkt $1 \cdot 2 \cdot 3 \cdots x$ reducirt; im letzten Falle fällt sie mit der im Vorhergehenden betrachteten Function zusammen.

Man gelangt sehr leicht zur Vorstellung der allgemeinen Functionen Γ, wenn man die Function $1 \cdot 2 \cdot 3 \cdots x$ zu interpoliren, d. h. wenn man das Produkt $1 \cdot 2 \cdot 3 \cdots x$ durch eine Function von x darzustellen sucht, welche eine völlig bestimmte Bedeutung behält, wenn x aufhört, eine ganze positive Zahl zu sein.

Es seien x und m zwei ganze positive Zahlen. Die x Brüche

$$\frac{m}{m+1}, \quad \frac{m}{m+2}, \quad \ldots, \quad \frac{m}{m+x}$$

nähern sich der Einheit, wenn m unbegrenzt wächst, während x constant bleibt. Dasselbe ist daher mit dem Produkte dieser x Brüche der Fall, und man hat

$$\frac{m^x}{(m+1)\,(m+2)\cdots(m+x)}\,(1+\varepsilon_m) = 1\,,$$

wo ε_m eine für $m = \infty$ verschwindende Grösse bezeichnet.

Man kann auch

$$\frac{(1 \cdot 2 \cdot 3 \cdots m)\, m^x}{1 \cdot 2 \cdot 3 \cdots (m+x)}\,(1+\varepsilon_m) = 1$$

schreiben, oder wenn man beide Glieder mit $1 \cdot 2 \cdot 3 \cdots x$ multiplicirt,

$$1 \cdot 2 \cdot 3 \cdots x = \frac{(1 \cdot 2 \cdot 3 \cdots m)\, m^x}{(x+1)\,(x+2)\cdots(x+m)}\,(1+\varepsilon_m)\,.$$

Lässt man jetzt die ganze Zahl m unendlich gross werden, so folgt

$$(1). \qquad 1 \cdot 2 \cdot 3 \cdots x = \lim_{m=\infty} \frac{(1 \cdot 2 \cdot 3 \cdots m)\, m^x}{(x+1)\,(x+2)\cdots(x+m)}\,.$$

Das zweite Glied dieser Formel wird unendlich, wenn x eine negative ganze Zahl ist; für alle übrigen reellen oder complexen Werthe von x hat es aber einen endlichen und bestimmten Werth, wie sich leicht nachweisen lässt. Setzt man daher

$$(2). \qquad \Gamma(x+1) = \lim_{m=\infty} \frac{(1 \cdot 2 \cdot 3 \cdots m)\, m^x}{(x+1)\,(x+2)\cdots(x+m)}\,,$$

so ist im Falle eines ganzen positiven x

$$\Gamma(x+1) = 1 \cdot 2 \cdot 3 \cdots x\,.$$

Für die folgende Betrachtung ist es nöthig, den Werth von $\Gamma(\frac{1}{2})$ zu bestimmen.

Macht man in der Formel (2) $x = -\frac{1}{2}$, so ergiebt sich

$$\Gamma(\tfrac{1}{2}) = \lim_{m=\infty} \frac{(1 \cdot 2 \cdot 3 \cdots m)^2 \, 2^{2m} \, m^{-\frac{1}{2}}}{1 \cdot 2 \cdot 3 \cdots 2m},$$

oder, wenn wie in No. 378

$$\varphi(m) = \frac{1 \cdot 2 \cdot 3 \cdots m}{\sqrt{2\pi} \cdot e^{-m} \cdot m^{m+\frac{1}{2}}}$$

gesetzt wird,

$$\Gamma(\tfrac{1}{2}) = \lim_{m=\infty} \sqrt{\pi} \cdot \frac{[\varphi(m)]^2}{\varphi(2m)}.$$

Da endlich jede der Grössen $\varphi(m)$, $\varphi(2m)$ für $m = \infty$ sich auf Eins reducirt, so ist

$$\Gamma(\tfrac{1}{2}) = \sqrt{\pi}.$$

383. Nach dem Vorhergehenden kann man

$$(1). \qquad \Gamma(x+1) = \frac{1 \cdot 2 \cdot 3 \cdots m) \, m^x}{(x+1)(x+2)\cdots(x+m)} (1 + \varepsilon_m)$$

schreiben, wo ε_m eine für $m = \infty$ verschwindende Grösse ist. Aus dieser Formel folgt

$$\log \Gamma(x+1) = \left[x \log \frac{2}{1} - \log \frac{x+1}{1}\right] + \cdots$$
$$+ \left[x \log \frac{m}{m-1} - \log \frac{x+m}{m}\right] + \log(1 + \varepsilon_m),$$

oder, wenn man $m+2$ statt m schreibt, und m unendlich gross werden lässt,

$$(2). \qquad \log \Gamma(x+1) = \sum_{m=0}^{m=\infty} \left[x \log\left(1 + \frac{1}{m+1}\right) - \log\left(1 + \frac{x}{m+1}\right)\right].$$

Diese Formel ist mit (1) gleichbedeutend und enthält gleichfalls die allgemeine Definition der Functionen Γ.

Es ist jetzt leicht, die Allgemeinheit der Formel (18) der No. 380 nachzuweisen; dieselbe liefert nämlich, ebenso wie die vorhergehende Formel, wenn man zweimal nach x differentiirt,

$$\frac{d^2 \log \Gamma(x+1)}{dx^2} = \sum_{m=0}^{m=\infty} \frac{1}{(x+m+1)^2}.$$

Da demnach die ersten Glieder beider Formeln dieselbe Abge-

leitete zweiter Ordnung haben, so können sie sich nur durch eine lineare Function von x von einander unterscheiden. Nun sind sie aber für alle ganzen und positiven Werthe von x einander gleich; folglich müssen sie für alle Werthe von x gleich sein.

384. Wir können nicht umhin, darauf aufmerksam zu machen, dass die Function $\Gamma(x)$ für positive Werthe von x nichts Anderes ist, als die Function, welche von Legendre den Namen: Eulersches Integral zweiter Art erhalten hat. Schreibt man nämlich $x-1$ statt x, so geht die Formel (1) der vorhergehenden Nummer über in

$$\Gamma(x) = \lim_{m=\infty} \frac{(1\cdot 2\cdot 3\cdots m)\, m^{x-1}}{x\,(x+1)\cdots(x+m-1)}.$$

Durch theilweise Integration des Differentials $\alpha^{x-1}(1-\alpha)^m d\alpha$ ergiebt sich

$$\int \alpha^{x-1}(1-\alpha)^m d\alpha = \frac{\alpha^x(1-\alpha)^m}{x} + \frac{m}{x}\int \alpha^x(1-\alpha)^{m-1} d\alpha,$$

und wenn man die Integrationsgrenzen 0 und 1 nimmt, so erhält man, da x positiv ist,

$$\int_0^1 \alpha^{x-1}(1-\alpha)^m d\alpha = \frac{m}{x}\int_0^1 \alpha^x(1-\alpha)^{m-1} d\alpha.$$

Daraus geht hervor, dass für jeden Werth der ganzen Zahl n

$$\int_0^1 \alpha^{x-1}(1-\alpha)^m d\alpha = \frac{m(m-1)\cdots(m-n+1)}{x(x+1)\cdots(x+n-1)}\int_0^1 \alpha^{x+n-1}(1-\alpha)^{m-n} d\alpha$$

ist. Für $m=n$ reducirt sich das Integral des zweiten Gliedes auf

$$\int_0^1 \alpha^{x+m-1} d\alpha = \frac{1}{x+m};$$

man hat daher

$$\int_0^1 \alpha^{x-1}(1-\alpha)^m d\alpha = \frac{1\cdot 2\cdot 3\cdots m}{x\,(x+1)\cdots(x+m)},$$

und, wenn $\frac{\alpha}{m}$, $\frac{d\alpha}{m}$ statt α, $d\alpha$ geschrieben wird,

$$\frac{x+m}{m}\int_0^m \alpha^{x-1}\left(1-\frac{\alpha}{m}\right)^m d\alpha = \frac{(1\cdot 2\cdot 3\cdots m)\, m^{x-1}}{x\,(x+1)\cdots(x+m-1)}.$$

Danach ist

$$\Gamma(x) = \lim_{m=\infty} \left(1 + \frac{x}{m}\right) \int_0^m \alpha^{x-1} \left(1 - \frac{\alpha}{m}\right)^m d\alpha,$$

oder auch

$$\Gamma(x) = \lim_{m=\infty} \left(1 + \frac{x}{m}\right) \left[\int_0^M \alpha^{x-1} \left(1 - \frac{\alpha}{m}\right)^m d\alpha \right.$$

$$\left. + \int_M^m \alpha^{x-1} \left(1 - \frac{\alpha}{m}\right)^m d\alpha \right].$$

Die Grösse $\left(1 - \frac{\alpha}{m}\right)^m$ hat den Logarithmus

$$-\left(\alpha + \frac{\alpha^2}{2m} + \frac{\alpha^3}{3m^2} + \cdots\right)$$

und erreicht ihr Maximum, wenn α als constant angesehen wird, für $m = \infty$; dieses Maximum ist $e^{-\alpha}$. Es ist daher

$$\int_M^m \alpha^{x-1} \left(1 - \frac{\alpha}{m}\right)^m d\alpha < \int_M^m \alpha^{x-1} e^{-\alpha} d\alpha,$$

und man kann

$$\int_M^m \alpha^{x-1} \left(1 - \frac{\alpha}{m}\right)^m d\alpha = (1 - \vartheta) \int_M^m \alpha^{x-1} e^{-\alpha} d\alpha$$

setzen, worin $0 < \vartheta < 1$ vorausgesetzt wird. Der Ausdruck von $\Gamma(x)$ geht dann über in

$$\Gamma(x) = \lim_{m=\infty} \left(1 + \frac{x}{m}\right) \left[\int_0^M \alpha^{x-1} \left(1 - \frac{\alpha}{m}\right)^m d\alpha \right.$$

$$\left. + (1 - \vartheta) \int_M^m \alpha^{x-1} e^{-\alpha} d\alpha \right].$$

Wir sehen jetzt M als constant an und lassen m unendlich gross werden; für $m = \infty$ ist $\left(1 - \frac{\alpha}{m}\right)^m = e^{-\alpha}$, folglich

$$\Gamma(x) = \int_0^\infty \alpha^{x-1} e^{-\alpha} d\alpha - \vartheta \int_M^\infty \alpha^{x-1} e^{-\alpha} d\alpha.$$

Es liegt aber auf der Hand, dass ϑ hier in aller Strenge Null sein muss; denn die vorhergehende Formel besteht für jeden Werth von M, und der letzte Theil verschwindet für $M = \infty$. Man hat mithin für alle positiven Werthe von x

$$\Gamma(x) = \int_0^\infty \alpha^{x-1} e^{-\alpha} d\alpha.$$

Bestimmung zweier Grenzen für die Summe der natürlichen Logarithmen aller ganzen Zahlen, die nicht grösser als eine gegebene Zahl sind.

385. Es sei a eine positive ganze Zahl. Wir machen in der Formel (19) der No. 381 $x = a + 1$ und subtrahiren sodann von jedem Gliede $\log (a + 1)$. Zugleich machen wir in der Formel (20) derselben Nummer $x = a$; dadurch erhalten wir

$$(1). \begin{cases} \log 1 \,.\, 2 \,.\, 3 \ldots a > \log \sqrt{2\pi} + (a+1) \log (a+1) - (a+1) - \frac{1}{2} \log(a+1), \\ \log 1 \,.\, 2 \,.\, 3 \ldots a < \log \sqrt{2\pi} + a \log a - a + \frac{1}{2} \log a + \frac{1}{12a}. \end{cases}$$

Dies vorausgesetzt, sei x eine beliebige positive Grösse, die wenigstens gleich 1 ist, und es bezeichne a die grösste in x enthaltene ganze Zahl. Der Voraussetzung nach hat man

$$a \leqq x < a + 1 \text{ und } a \geqq 1;$$

daraus folgt

$$\left(a + 1 - \frac{1}{2}\right) \left[\log (a + 1) - 1\right] > \left(x - \frac{1}{2}\right) (\log x - 1),$$

$$\left(a + \frac{1}{2}\right) (\log a - 1) + \frac{1}{12a} \overline{\overline{<}} \left(x + \frac{1}{2}\right) (\log x - 1) + \frac{1}{12},$$

oder

$$(2). \begin{cases} (a + 1) \log (a + 1) - (a + 1) - \frac{1}{2} \log (a + 1) \\ \qquad\qquad > x \log x - x - \frac{1}{2} \log x, \\ a \log a - a + \frac{1}{2} \log a + \frac{1}{12a} \\ \qquad\qquad \overline{\overline{<}} x \log x - x + \frac{1}{2} \log x + \frac{1}{12}. \end{cases}$$

Nennt man $T(x)$ den Logarithmus des Produkts aller ganzen Zahlen, die nicht grösser als x sind, so ergiebt sich aus den Ungleichungen (1) und (2)

$$(3). \quad \begin{cases} T(x) > \log \sqrt{2\pi} + x \log x - x - \frac{1}{2} \log x, \\ T(x) < \log \sqrt{2\pi} + x \log x - x + \frac{1}{2} \log x + \frac{1}{12}, \end{cases}$$

und dies sind die Ungleichungen, die wir herleiten wollten.

Ueber die Anzahl der zwischen zwei gegebenen Grenzen enthaltenen Primzahlen.

386. Die Aufgabe, die Anzahl der Primzahlen zu bestimmen, welche zwischen zwei gegebenen Zahlen liegen, ist noch nicht gelöst worden und scheint die grössten Schwierigkeiten darzubieten. Tchebichef ist der erste, der diese Frage mit Erfolg behandelt hat. In einer 1850 der Petersburger Akademie vorgelegten Arbeit lehrt er, die Zahl, welche die Anzahl der zwischen zwei gegebenen Grenzen enthaltenen Primzahlen angiebt, zwischen zwei Grenzen einzuschliessen. Aus seiner Betrachtung leitet Tchebichef sodann den Beweis eines Postulats her, auf welches Bertrand den Beweis eines wichtigen Lehrsatzes gegründet hatte, den wir im nächsten Theile dieses Werkes kennen lernen werden. Dieses Postulat besteht im Folgenden:

Wenn $a > \frac{7}{2}$ ist, so liegt zwischen a und $2a - 2$ immer wenigstens eine Primzahl.

Obwohl es mir, wie man im 4ten Theile sehen wird, gelungen ist, den in Rede stehenden Satz zu beweisen, ohne irgend ein Postulat zu Hilfe zu nehmen, so halte ich es doch für zweckmässig, die geistreiche, auf völlig neuen Betrachtungen beruhende Untersuchung von Tchebichef hier mitzutheilen.

Wir bezeichnen, wie im Vorhergehenden, mit $T(z)$ die Summe der natürlichen Logarithmen aller ganzen Zahlen, die nicht grösser als z sind. Ausserdem bezeichne $\vartheta(z)$ die Summe der natürlichen Logarithmen aller Primzahlen, die nicht grösser als z sind. Die Functionen $T(z)$ und $\vartheta(z)$ reduciren sich auf Null, wenn $z < 2$ ist. Wenn z eine zusammengesetzte Grösse, z. B. $\left(\frac{x}{2}\right)^{\frac{1}{2}}$ ist, so schreiben wir der Kürze wegen $\vartheta\left(\frac{x}{2}\right)^{\frac{1}{2}}$ statt $\vartheta\left[\left(\frac{x}{2}\right)^{\frac{1}{2}}\right]$.

Fundamental-Eigenschaft der Function $\vartheta(z)$.

387. Die Fundamental-Eigenschaft, auf welcher Tchebichef's Untersuchung beruht, besteht in folgender Formel:

$$
\begin{aligned}
T(x) = \vartheta(x) &+ \vartheta(x)^{\frac{1}{2}} + \vartheta(x)^{\frac{1}{3}} + \vartheta(x)^{\frac{1}{4}} + \cdots \\
&+ \vartheta\left(\frac{x}{2}\right) + \vartheta\left(\frac{x}{2}\right)^{\frac{1}{2}} + \vartheta\left(\frac{x}{2}\right)^{\frac{1}{3}} + \vartheta\left(\frac{x}{2}\right)^{\frac{1}{4}} + \cdots \\
&+ \vartheta\left(\frac{x}{3}\right) + \vartheta\left(\frac{x}{3}\right)^{\frac{1}{2}} + \vartheta\left(\frac{x}{3}\right)^{\frac{1}{3}} + \vartheta\left(\frac{x}{3}\right)^{\frac{1}{4}} + \cdots \\
&+ \vartheta\left(\frac{x}{4}\right) + \vartheta\left(\frac{x}{4}\right)^{\frac{1}{2}} + \vartheta\left(\frac{x}{4}\right)^{\frac{1}{3}} + \vartheta\left(\frac{x}{4}\right)^{\frac{1}{4}} + \cdots \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ;
\end{aligned}
$$

darin müssen die Reihen bis zu den Termen fortgesetzt werden, die sich gleich Null ergeben.

Um diese Formel zu beweisen, bemerken wir, dass jedes Glied gleich ist einer Summe von Termen, wie $k \log \alpha$, worin k eine ganze Zahl und α eine Primzahl bezeichnet. Setzen wir nun voraus, dass in der Reihe der Zahlen 1, 2, 3, 4, ..., die nicht grösser als x sind, es A_1 Zahlen giebt, die durch α, A_2 Zahlen, die durch α^2, allgemein A_i Zahlen, die durch α^i theilbar sind, so hat $\log \alpha$ in $T(x)$ offenbar den Coefficienten

$$A_1 + A_2 + A_3 + \cdots.$$

Betrachten wir jetzt die Terme, welche eine Verticalreihe des zweiten Gliedes unserer Formel ausmachen, z. B.

$$\vartheta(x)^{\frac{1}{i}}, \quad \vartheta\left(\frac{x}{2}\right)^{\frac{1}{i}}, \quad \vartheta\left(\frac{x}{3}\right)^{\frac{1}{i}}, \quad \vartheta\left(\frac{x}{4}\right)^{\frac{1}{i}}, \ldots.$$

In dieser Reihe kommen ebenso viele Terme vor, welche $\log \alpha$ mit dem Coefficienten 1 enthalten, als die Reihe

$$x^{\frac{1}{i}}, \left(\frac{x}{2}\right)^{\frac{1}{i}}, \left(\frac{x}{3}\right)^{\frac{1}{i}}, \left(\frac{x}{4}\right)^{\frac{1}{i}}, \ldots$$

Grössen enthält, die nicht kleiner als α sind. Die Anzahl dieser Grössen stimmt augenscheinlich mit der Anzahl der Grössen

$$\alpha^i, \; 2\alpha^i, \; 3\alpha^i, \; 4\alpha^i, \ldots$$

überein, die nicht grösser als x sind; diese Anzahl ist genau diejenige Zahl, die wir mit A_i bezeichnet haben. Der Coefficient von $\log \alpha$ im zweiten Gliede unserer Formel ist somit

$$A_1 + A_2 + A_3 + \cdots,$$

und dies beweist die Richtigkeit dieser Formel.

Wir werden der Kürze wegen

(1). $\psi(z) = \vartheta(z) + \vartheta(z)^{\frac{1}{2}} + \vartheta(z)^{\frac{1}{3}} + \vartheta(z)^{\frac{1}{4}} + \cdots$

machen; dann lässt sich die eben bewiesene Formel in folgender Weise schreiben:

(2). $T(x) = \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \psi\left(\frac{x}{4}\right) + \cdots.$

Beweis zweier Ungleichungen, denen die Function $\psi(z)$ genügt.

388. Die beiden Ungleichungen, die wir herleiten wollen, sind folgende:

$$\psi(x) > T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right),$$

$$\psi(x) - \psi\left(\frac{x}{6}\right) < T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right).$$

Die Gleichung (2) der No. 387 liefert:

$$(1).\quad \begin{cases} T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) \\ = \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \psi\left(\frac{x}{4}\right) + \cdots \\ + \psi\left(\frac{x}{30}\right) + \psi\left(\frac{x}{2\,.\,30}\right) + \psi\left(\frac{x}{3\,.\,30}\right) + \psi\left(\frac{x}{4\,.\,30}\right) + \cdots \\ - \psi\left(\frac{x}{2}\right) - \psi\left(\frac{x}{2\,.\,2}\right) - \psi\left(\frac{x}{3\,.\,2}\right) - \psi\left(\frac{x}{4\,.\,2}\right) - \cdots \\ - \psi\left(\frac{x}{3}\right) - \psi\left(\frac{x}{2\,.\,3}\right) - \psi\left(\frac{x}{3\,.\,3}\right) - \psi\left(\frac{x}{4\,.\,3}\right) - \cdots \\ - \psi\left(\frac{x}{5}\right) - \psi\left(\frac{x}{2\,.\,5}\right) - \psi\left(\frac{x}{3\,.\,5}\right) - \psi\left(\frac{x}{4\,.\,5}\right) - \cdots \end{cases}$$

Das zweite Glied dieser Gleichung hat die Form

$$A_1\,\psi(x) + A_2\,\psi\left(\frac{x}{2}\right) + A_3\,\psi\left(\frac{x}{3}\right) + \cdots + A_n\,\psi\left(\frac{x}{n}\right) + \cdots,$$

wo $A_1, A_2, A_3, \ldots$ ganze Coefficienten sind. Wir behaupten nun, es sei allgemein

$A_n = 1$, wenn n durch k e i n e der Zahlen 2, 3, 5 theilbar ist,
$A_n = 0$, wenn n durch n u r e i n e der Zahlen 2, 3, 5 theilbar ist,
$A_n = -1$, wenn n durch w e n i g s t e n s z w e i der Zahlen 2, 3, 5 theilbar ist.

Ist nämlich n durch keine der Zahlen 2, 3, 5 theilbar, so steht der Term $\psi\left(\frac{x}{n}\right)$ nur in der ersten Horizontalreihe des zweiten Gliedes der Formel (1).

Ist n durch eine, aber auch nur eine der Zahlen 2, 3, 5 theilbar, so steht der Term $\psi\left(\frac{x}{n}\right)$ mit dem Zeichen — in einer der drei letzten Horizontalreihen und mit dem Zeichen + in der ersten Horizontalreihe des zweiten Gliedes der Gleichung (1); der Coefficient von $\psi\left(\frac{x}{n}\right)$ reducirt sich folglich in diesem Falle auf Null.

Wenn n durch zwei der Zahlen 2, 3, 5 theilbar ist, so findet sich der Term $\psi\left(\frac{x}{n}\right)$ mit dem Zeichen + in der ersten, mit dem Zeichen — in zweien der drei letzten Horizontalreihen des zweiten Gliedes von (1) vor; sein Coefficient reducirt sich daher auf — 1.

Wenn endlich n durch jede der drei Zahlen 2, 3, 5 theilbar ist, so steht der Term $\psi\left(\frac{x}{n}\right)$ in den beiden ersten Horizontalreihen des zweiten Gliedes von (1) mit dem Zeichen +, in den drei letzten Reihen mit dem Zeichen —; sein Coefficient ist somit — 1. Den Werthen von n

$$n = 30\,m + \begin{array}{l} 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10, \\ 11,\ 12,\ 13,\ 14,\ 15,\ 16,\ 17,\ 18,\ 19,\ 20, \\ 21,\ 22,\ 23,\ 24,\ 25,\ 26,\ 27,\ 28,\ 29,\ 30 \end{array}$$

entsprechen danach folgende Werthe von A_n

$$A_n = \begin{array}{l} 1,\ 0,\ 0,\ 0,\ 0,\ -1,\ 1,\ 0,\ 0,\ -1, \\ 1,\ -1,\ 1,\ 0,\ -1,\ 0,\ 1,\ -1,\ 1,\ -1, \\ 0,\ 0,\ 1,\ -1,\ 0,\ 0,\ 0,\ 0,\ 1,\ -1, \end{array}$$

und folglich reducirt sich die Gleichung (1) auf

$$T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right)$$

$$= \psi(x) - \psi\left(\frac{x}{6}\right) + \psi\left(\frac{x}{7}\right) - \psi\left(\frac{x}{10}\right) + \psi\left(\frac{x}{11}\right) - \psi\left(\frac{x}{12}\right) + \cdots;$$

alle Terme des zweiten Gliedes dieser Formel haben abwechselnd + 1 und — 1 zum Coefficienten. Nun kann die Function $\psi(z)$ nicht wachsen, wenn z abnimmt; mithin ist die Reihe

$$\psi(x) - \psi\left(\frac{x}{6}\right) + \psi\left(\frac{x}{7}\right) - \psi\left(\frac{x}{10}\right) + \cdots,$$

welche das zweite Glied der vorhergehenden Formel ausmacht, zwischen

$$\psi(x) \text{ und } \psi(x) - \psi\left(\frac{x}{6}\right)$$

enthalten, und man hat, wie zu beweisen war,

$$(2). \begin{cases} \psi(x) \geqq T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) \\ \psi(x) - \psi\left(\frac{x}{6}\right) < T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right). \end{cases}$$

Bestimmung zweier Grenzen, zwischen welchen die Functionen $\psi(z)$ und $\vartheta(z)$ enthalten sind.

389. In No. 385 hat man gesehen, dass die Function $T(x)$ den beiden folgenden Ungleichungen genügt:

$$(1). \begin{cases} T(x) < \log\sqrt{2\pi} + x\log x - x + \frac{1}{2}\log x + \frac{1}{12}, \\ T(x) > \log\sqrt{2\pi} + x\log x - x - \frac{1}{2}\log x. \end{cases}$$

Daraus ergiebt sich

$$T(x) + T\left(\frac{x}{30}\right) < 2\log\sqrt{2\pi}$$

$$+ \frac{2}{12} + \frac{31}{30}x\log x - x\log 30^{\frac{1}{30}} - \frac{31}{30}x + \log x - \frac{1}{2}\log 30,$$

$$T(x) + T\left(\frac{x}{30}\right) > 2\log\sqrt{2\pi}$$

$$+ \frac{31}{30}x\log x - x\log 30^{\frac{1}{30}} - \frac{31}{30}x - \log x + \frac{1}{2}\log 30,$$

und weiter

$$T\left(\frac{x}{2}\right) + T\left(\frac{x}{3}\right) + T\left(\frac{x}{5}\right) < 3\log\sqrt{2\pi} + \frac{3}{12}$$

$$+ \frac{31}{30}x\log x - x\log 2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}} - \frac{31}{30}x + \frac{3}{2}\log x - \frac{1}{2}\log 30,$$

$$T\left(\frac{x}{2}\right) + T\left(\frac{x}{3}\right) + T\left(\frac{x}{5}\right) > 3\log\sqrt{2\pi}$$

$$+ \frac{31}{30}x\log x - x\log 2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}} - \frac{31}{30}x - \frac{3}{2}\log x + \frac{1}{2}\log 30.$$

Wird die vierte dieser Ungleichungen von der ersten und die dritte von der zweiten subtrahirt, so folgt

$$T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right)$$

$$< x \log \frac{2^{\frac{1}{2}}\, 3^{\frac{1}{3}}\, 5^{\frac{1}{5}}}{30^{\frac{1}{30}}} + \frac{5}{2} \log x - \frac{1}{2} \log 1800\pi + \frac{2}{12},$$

$$T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right)$$

$$> x \log \frac{2^{\frac{1}{2}}\, 3^{\frac{1}{3}}\, 5^{\frac{1}{5}}}{30^{\frac{1}{30}}} - \frac{5}{2} \log x + \frac{1}{2} \log \frac{450}{\pi} - \frac{3}{12}.$$

Machen wir der Kürze wegen

$$A = \log \frac{2^{\frac{1}{2}}\, 3^{\frac{1}{3}}\, 5^{\frac{1}{5}}}{30^{\frac{1}{30}}} = 0{,}92129202\ldots,$$

so gehen die letzten Ungleichungen über in

$$(2). \begin{cases} T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) \\ \qquad < Ax + \frac{5}{2} \log x - \frac{1}{2} \log 1800\pi + \frac{2}{12}, \\ T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) \\ \qquad > Ax - \frac{5}{2} \log x + \frac{1}{2} \log \frac{450}{\pi} - \frac{3}{12}. \end{cases}$$

Es ist also um so mehr

$$(3). \begin{cases} T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) < Ax + \frac{5}{2} \log x, \\ T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) > Ax - \frac{5}{2} \log x - 1. \end{cases}$$

Die Formeln (1) finden nur dann statt, wenn $x > 1$ ist. Um ferner die Ungleichungen (2) zu bilden, hat man x durch $\frac{x}{2}$, $\frac{x}{3}$, $\frac{x}{5}$, $\frac{x}{30}$ ersetzt; folglich setzt das Bestehen der Formeln (2) $x > 30$ voraus. Es ist aber leicht zu zeigen, dass die Formeln (3) für alle zwischen 1 und 30 enthaltenen Werthe von x, also allgemein gültig sind.

Verbindet man die Ungleichungen (3) mit den Ungleichungen (2) der No. 388, so erhält man

$$(4).\quad \begin{cases} \psi(x) > \quad A\,x - \frac{5}{2}\log x - 1\,, \\ \psi(x) - \psi\left(\frac{x}{6}\right) < A\,x + \frac{5}{2}\log x. \end{cases}$$

Die erste dieser Formeln liefert unmittelbar eine untere Grenze von $\psi(x)$; die zweite soll uns jetzt zur Ermittlung einer oberen Grenze dienen:

Wir setzen

$$f(x) = \frac{6}{5}\,A\,x + \frac{5}{4\log 6}\log^2 x + \frac{5}{4}\log x;$$

dann ist

$$f\left(\frac{x}{6}\right) = \frac{1}{5}\,A\,x + \frac{5}{4\log 6}\log^2 x - \frac{5}{4}\log x\,,$$

folglich

$$f(x) - f\left(\frac{x}{6}\right) = A\,x + \frac{5}{2}\log x,$$

und

$$\psi(x) - \psi\left(\frac{x}{6}\right) < f(x) - f\left(\frac{x}{6}\right),$$

$$\psi(x) - f(x) \quad < \psi\left(\frac{x}{6}\right) - f\left(\frac{x}{6}\right).$$

Setzt man der Reihe nach $\frac{x}{6}, \frac{x}{6^2}, \frac{x}{6^3}, \ldots, \frac{x}{6^{m+1}}$ statt x, so folgt aus der letzten Ungleichung

$$(5).\quad \begin{cases} \psi(x) - f(x) < \psi\left(\frac{x}{6}\right) - f\left(\frac{x}{6}\right) < \psi\left(\frac{x}{6^2}\right) - f\left(\frac{x}{6^2}\right) < \cdots \\ \qquad < \psi\left(\frac{x}{6^{m+1}}\right) - f\left(\frac{x}{6^{m+1}}\right). \end{cases}$$

Es sei jetzt m die grösste ganze Zahl, welche der Bedingung $6^m \overline{\overline{<}}\, x$ genügt; dann liegt $\frac{x}{6^{m+1}}$ zwischen 1 und $\frac{1}{6}$, folglich ist $\psi\left(\frac{x}{6^{m+1}}\right) = 0$. Ausserdem behaupten wir, dass $-f\left(\frac{x}{6^{m+1}}\right) < 1$ ist. Der Werth von $-f(z)$ kann nämlich in folgender Weise geschrieben werden:

$$-f(z) = \frac{5\log 6}{16} - \frac{5}{4\log 6}\left(\log z + \tfrac{1}{2}\log 6\right)^2 - \frac{6}{5}\,A\,z;$$

daraus geht hervor, dass

$$-f(z) < \frac{5\log 6}{16},$$

und um so mehr

$$-f(z) < 1$$

ist; denn 6 ist kleiner als e^3, also $\log 6 < 3$.

Die Formel (5) liefert danach

$$\psi(x) - f(x) < 1,$$

folglich

$$(6). \qquad \psi(x) < \frac{6}{5} A x + \frac{5}{4 \log 6} \log^2 x + \frac{5}{4} \log x + 1.$$

Die für $\psi(x)$ gefundenen Grenzen setzen uns in den Stand, auch die Function $\vartheta(x)$ in zwei Grenzen einzuschliessen;

Aus der Formel

$$\psi(z) = \vartheta(z) + \vartheta(z)^{\frac{1}{2}} + \vartheta(z)^{\frac{1}{3}} + \cdots$$

folgt

$$\psi(x) - \psi\left(\sqrt{x}\right) = \vartheta(x) + \vartheta(x)^{\frac{1}{3}} + \vartheta(x)^{\frac{1}{5}} + \vartheta(x)^{\frac{1}{7}} + \cdots,$$

$$\psi(x) - 2\psi\left(\sqrt{x}\right)$$

$$= \vartheta(x) - \left[\vartheta(x)^{\frac{1}{2}} - \vartheta(x)^{\frac{1}{3}}\right] - \left[\vartheta(x)^{\frac{1}{4}} - \vartheta(x)^{\frac{1}{5}}\right] - \cdots.$$

Nun ist die Function $\vartheta(z)$ positiv oder Null; ferner kann sie nicht wachsen, während z abnimmt; man hat somit

$$(7). \qquad \begin{cases} \vartheta(x) \overline{\overline{<}} \psi(x) - \psi\left(\sqrt{x}\right), \\ \vartheta(x) \overline{\overline{>}} \psi(x) - 2\psi\left(\sqrt{x}\right). \end{cases}$$

Wir haben aber eben die Ungleichungen

$$(8). \qquad \begin{cases} \psi(x) < \frac{6}{5} A x + \frac{5}{4 \log 6} \log^2 x + \frac{5}{4} \log x + 1, \\ \psi(x) > A x - \frac{5}{2} \log x - 1 \end{cases}$$

hergeleitet, aus denen

$$(9). \qquad \begin{cases} \psi\left(\sqrt{x}\right) < \frac{6}{5} A x^{\frac{1}{2}} + \frac{5}{16 \log 6} \log^2 x + \frac{5}{8} \log x + 1, \\ \psi\left(\sqrt{x}\right) > A x^{\frac{1}{2}} - \frac{5}{4} \log x - 1 \end{cases}$$

hervorgeht; mithin liefern die Ungleichungen (7):

$$(10). \qquad \begin{cases} \vartheta(x) < \frac{6}{5} A x - A x^{\frac{1}{2}} + \frac{5}{4 \log 6} \log^2 x + \frac{5}{2} \log x + 2, \\ \vartheta(x) > A x - \frac{12}{5} A x^{\frac{1}{2}} - \frac{5}{8 \log 6} \log^2 x - \frac{15}{4} \log x - 3, \end{cases}$$

und diese Formeln geben uns die Grenzen an, zwischen denen die Summe der Logarithmen aller Primzahlen enthalten ist, die nicht grösser als x sind.

Bestimmung zweier Grenzen für die Zahl, welche anzeigt, wie viele Primzahlen zwischen zwei gegebenen Zahlen liegen.

390. Es sei m die Anzahl der Primzahlen, welche grösser als eine gegebene Zahl l, aber nicht grösser als eine zweite gegebene Zahl L sind. Die Summe der natürlichen Logarithmen dieser m Primzahlen ist offenbar zwischen $m \log l$ und $m \log L$ enthalten, d. h. es ist

$$\vartheta(L) - \vartheta(l) > m \log l,$$
$$\vartheta(L) - \vartheta(l) < m \log L,$$

und folglich

$$m < \frac{\vartheta(L) - \vartheta(l)}{\log l}, \quad m > \frac{\vartheta(L) - \vartheta(l)}{\log L}.$$

Den Ungleichungen (10) der No. 389 zufolge hat man aber

$$\vartheta(L) - \vartheta(l) < A\left(\frac{6}{5} L - l\right) - A\left(L^{\frac{1}{2}} - \frac{12}{5} l^{\frac{1}{2}}\right)$$
$$+ \frac{5}{8 \log 6}(2 \log^2 L + \log^2 l) + \frac{5}{4}(2 \log L + 3 \log l) + 5,$$
$$\vartheta(L) - \vartheta(l) > A\left(L - \frac{6}{5} l\right) - A\left(\frac{12}{5} L^{\frac{1}{2}} - l^{\frac{1}{2}}\right)$$
$$- \frac{5}{8 \log 6}(\log^2 L + 2 \log^2 l) - \frac{5}{4}(3 \log L + 2 \log l) - 5,$$

also

$$(1). \left\{\begin{aligned} m &< \frac{1}{\log l}\Big\{A\left(\frac{6}{5} L - l\right) - A\left(L^{\frac{1}{2}} - \frac{12}{5} l^{\frac{1}{2}}\right) \\ &\quad + \frac{5}{8 \log 6}(2 \log^2 L + \log^2 l) + \frac{5}{4}(2 \log L + 3 \log l) + 5\Big\}, \\ m &> \frac{1}{\log L}\Big\{A\left(L - \frac{6}{5} l\right) - A\left(\frac{12}{5} L^{\frac{1}{2}} - l^{\frac{1}{2}}\right) \\ &\quad - \frac{5}{8 \log 6}(\log^2 L + 2 \log^2 l) - \frac{5}{4}(3 \log L + 2 \log l) - 5\Big\}. \end{aligned}\right.$$

Diese Formeln liefern zwei Grenzen, zwischen welchen die Grösse m, d. h. die Anzahl der Primzahlen liegt, die grösser als l, aber nicht grösser als L sind. Die zweite dieser Formeln lehrt, dass

zwischen l und L jedenfalls mehr als k Primzahlen liegen, wenn die folgende Bedingung erfüllt ist:

$$(2).\quad k < \frac{1}{\log L}\Big\{A\left(L-\frac{6}{5}l\right)-A\left(\frac{12}{5}L^{\frac{1}{2}}-l^{\frac{1}{2}}\right)$$
$$-\frac{5}{8\log 6}(\log^2 L+2\log^2 l)-\frac{5}{4}(3\log L+2\log l)-5\Big\},$$

und da $0 < l < L$ ist, so wird dieser Ungleichung durch den Werth:

$$k=\frac{A\left(L-\frac{6}{5}l\right)-\frac{12}{5}AL^{\frac{1}{2}}-\frac{15}{8\log 6}\log^2 L-\frac{25}{4}\log L-5}{\log L}$$

genügt, aus welchem

$$l=\frac{5}{6}L-2L^{\frac{1}{2}}-\frac{25}{16A\log 6}\log^2 L-\frac{5}{6A}\left(\frac{25}{4}+k\right)\log L-\frac{25}{6A}$$

folgt. Nimmt man diesen Werth für l, so ist man sicher, zwischen l und L mehr als k Primzahlen zu finden. Natürlich wird sowohl l als auch L grösser als 1 vorausgesetzt.

Macht man $k=0$, so ergiebt sich aus dem Vorhergehenden, dass zwischen l und L wenigstens eine Primzahl liegt, wenn l folgenden Werth hat:

$$(3).\quad l=\frac{5}{6}L-2L^{\frac{1}{2}}-\frac{25}{16A\log 6}\log^2 L-\frac{125\log L}{24A}-\frac{25}{6A}.$$

Anwendung der vorhergehenden Resultate.

391. Es ist leicht, aus den im Vorstehenden erhaltenen Resultaten den Beweis des Satzes zu entnehmen, von dem in No. 386 die Rede war. Wir haben uns nämlich soeben überzeugt, dass zwischen den Grenzen

$$\frac{5}{6}L-2L^{\frac{1}{2}}-\frac{25\log^2 L}{16A\log 6}-\frac{125\log L}{24A}-\frac{25}{6A}\ \text{und}\ L$$

wenigstens eine Primzahl enthalten ist. Um also zu beweisen, dass zwischen a und $2a-2$ wenigstens eine Primzahl liegt, hat man nur darzuthun, dass man durch einen geeigneten Werth von L den beiden folgenden Ungleichungen genügen kann:

$$2a-2 > L,$$

$$a < \frac{5}{6}L-2L^{\frac{1}{2}}-\frac{25\log^2 L}{16A\log 6}-\frac{125\log L}{24A}-\frac{25}{6A}.$$

Die erste dieser Ungleichungen wird offenbar durch den Werth

$$L = 2a - 3$$

befriedigt, für welchen die zweite in

$$a < \frac{5}{6}(2a - 3) - 2\sqrt{2a - 3} - \frac{25 \log^2 (2a - 3)}{16 A \log 6} - \frac{125 \log (2a - 3)}{24 A} - \frac{25}{6 A}$$

übergeht. Diese Ungleichung besteht für alle Werthe von a, welche grösser sind, als die grösste Wurzel der Gleichung

$$x = \frac{5}{6}(2x - 3) - 2\sqrt{2x - 3} - \frac{25 \log^2 (2x - 3)}{16 A \log 6} - \frac{125 \log (2x - 3)}{24 A} - \frac{25}{6 A}.$$

Diese grösste Wurzel liegt zwischen 159 und 160. Wenn also $a > 160$ ist, so giebt es jedenfalls eine Primzahl zwischen a und $2a - 2$. Was die unter 160 liegenden Werthe von a betrifft, so lässt sich der Satz unmittelbar mittels der Primzahltafeln bewahrheiten.

Vierter Theil.

Die Substitutionen.



Erstes Kapitel.

Allgemeine Eigenschaften der Substitutionen.

Permutationen gegebener Buchstaben und Substitutionen, durch welche man von einer Permutation zu einer anderen übergeht.

392. Die Permutationen der n Buchstaben

$$a, b, c, d, \ldots, k, l$$

sind die Resultate, die man erhält, wenn man diese Buchstaben auf alle möglichen Arten nebeneinander schreibt. In den Elementen der Algebra wird die Gesammtzahl N dieser Permutationen bestimmt; es ergiebt sich bekanntlich

$$N = 1 . 2 . 3 \ldots n.$$

Wir stellen die N Permutationen, um die es sich handelt, durch einfache Buchstaben

$$A_0, A_1, A_2, \ldots, A_{N-1}$$

dar. Die Operation, mittels welcher man von einer Permutation zu einer andern übergeht, heisst eine Substitution (No. 235). In Zukunft werden wir eine Substitution dadurch ausdrücken, dass wir die neue Permutation über die Permutation setzen, von der wir ausgehen, und beide einklammern. Danach bezeichnet das Symbol

$$\begin{pmatrix} A_1 \\ A_0 \end{pmatrix}$$

die Substitution, welche den Zweck hat, die Buchstaben der Permutation A_0 durch diejenigen zu ersetzen, welche beziehungsweise in A_1 dieselben Plätze einnehmen. Die Permutationen A_0 und A_1 sollen die Terme der Substitution, und zwar soll A_0 der Nenner, A_1 der Zähler heissen. Es liegt auf der

Hand, dass man zum Nenner einer gegebenen Substitution irgend eine der N Permutationen wählen kann.

Nimmt man A_0 als Nenner an, so erhält man alle Substitutionen dadurch, dass man der Reihe nach die N Permutationen zu Zählern macht; diese Substitutionen sind daher

$$\begin{pmatrix} A_0 \\ A_0 \end{pmatrix}, \begin{pmatrix} A_1 \\ A_0 \end{pmatrix}, \begin{pmatrix} A_2 \\ A_0 \end{pmatrix}, \ldots, \begin{pmatrix} A_{N-1} \\ A_0 \end{pmatrix}.$$

Das Symbol $\begin{pmatrix} A_0 \\ A_0 \end{pmatrix}$ drückt aus, dass die Reihenfolge der Buchstaben unverändert bleiben soll; es stellt, wie man sagt, eine identische Substitution dar. Es ist vortheilhaft, dies Symbol unter die Substitutionen aufzunehmen, deren Anzahl dann gleich N ist.

Die verschiedenen Substitutionen, die wir zu betrachten haben, werden wir oft durch einfache Buchstaben S, T, u. s. w. darstellen.

Wenn ein Buchstabe im Zähler und im Nenner einer Substitution denselben Platz einnimmt, so kann man ihn ohne Nachtheil unterdrücken. So lässt sich die Substitution

$$S = \begin{pmatrix} d\,b\,c\,a \ldots \\ a\,b\,c\,d \ldots \end{pmatrix}$$

einfacher in folgender Weise schreiben:

$$S = \begin{pmatrix} d\,a \ldots \\ a\,d \ldots \end{pmatrix}.$$

Man sagt, eine Substitution sei auf die einfachste Form gebracht, wenn in beiden Termen alle Buchstaben unterdrückt sind, welche darin dieselben Plätze einnahmen.

Produkte von Substitutionen.

393. Unter dem Produkt einer gegebenen Permutation in eine Substitution versteht man die neue Permutation, die man erhält, wenn man die Substitution auf die gegebene Permutation anwendet. Dies Produkt wird dadurch dargestellt, dass man die Substitution links neben die gegebene Permutation schreibt. Wendet man z. B. die Substitution

$$S = \begin{pmatrix} A_1 \\ A_0 \end{pmatrix}$$

auf die Permutation A_0 an, so erhält man die Permutation A_1, und wir schreiben folglich

$$SA_0 = \binom{A_1}{A_0} A_0 = A_1.$$

Unter dem **Produkt** zweier gegebenen Substitutionen versteht man die neue Substitution, welche dasselbe leistet, wie die beiden gegebenen Substitutionen, wenn dieselben nach einander auf irgend eine Permutation angewandt werden. Man stellt dieses Produkt dadurch dar, dass man die Substitution, welche zuerst ausgeführt werden soll, rechts neben die andere Substitution setzt. Sind demnach

$$S = \binom{A_1}{A_0}, \; T = \binom{A_2}{A_0}$$

zwei gegebene Substitutionen, so drückt das Produkt

$$TS \text{ oder } \binom{A_2}{A_0} \binom{A_1}{A_0}$$

aus, dass man erst die Substitution S, dann die Substitution T ausführen soll; umgekehrt ist es mit

$$ST \text{ oder } \binom{A_1}{A_0} \binom{A_2}{A_0}.$$

Wenn die beiden Produkte ST und TS einander gleich sind, so sagt man, die Substitutionen S und T seien **gegeneinander vertauschbar**. Von solcher Beschaffenheit sind offenbar zwei Substitutionen, deren einfachste Ausdrücke keinen Buchstaben gemeinschaftlich haben.

Das Produkt einer beliebigen Anzahl von Substitutionen $S, T, U, V, \ldots$ ist das Resultat, welches man erhält, wenn man die erste Substitution mit der zweiten, das so entstandene Produkt mit der dritten, u. s. w. multiplicirt; es wird durch

$$\ldots V\,U\,T\,S \text{ dargestellt.}$$

Wenn die in Rede stehenden Substitutionen, deren Anzahl ν sein möge, sämmtlich gleich S sind, so heisst das Produkt die ν^{te} Potenz von S und wird durch S^ν dargestellt.

Wenn in einem Produkte eine identische Substitution, wie $\binom{A_0}{A_0}$ enthalten ist, so kann sie unterdrückt werden, und es ist

folglich naturgemäss, dieselbe gleich Eins anzunehmen; wir schreiben somit

$$\binom{A_0}{A_0} = 1.$$

Ausserdem werden wir das Symbol S^ν als Eins betrachten, sobald ν sich auf Null reducirt, die Substitution S mag sein, welche sie wolle. Daraus folgt dann, dass die nullte Potenz jeder Substitution eine identische Substitution bezeichnet.

Ordnung einer Substitution.

394. Es sei S eine beliebige Substitution; die Reihe der Potenzen von S ist

$$S^0 \text{ oder } 1\,,\, S\,,\, S^2\,,\, S^3\,,\, \ldots\,,\, S^\nu\,,\, \ldots .$$

Da nun die Gesammtzahl der Substitutionen beschränkt ist, so müssen, wenn die vorhergehende Reihe hinlänglich weit fortgesetzt wird, bereits erhaltene Substitutionen wieder zum Vorschein kommen. Wir nehmen an, es sei

$$S^{\mu+\nu} = S^\mu\,,$$

oder, da $S^{\mu+\nu} = S^\nu S^\mu$ ist,

$$S^\nu S^\mu = S^\mu\,.$$

Diese Formel lehrt, dass die Anwendung der Substitution S^ν auf irgend eine Permutation durchaus keine Versetzung der Buchstaben zur Folge hat; mit andern Worten, diese Substitution ist eine identische, und man hat

$$S^\nu = 1.$$

Daraus schliesst man, dass für jeden Werth der ganzen Zahl q

$$(S^\nu)^q \text{ oder } S^{\nu q} = 1$$

ist, und durch Multiplication mit der r^{ten} Potenz von S folgt weiter

$$S^{\nu q + r} = S^r.$$

Danach bilden die Potenzen von S eine periodische Reihe, und zwar besteht die Periode aus den Substitutionen

$$1\,,\, S\,,\, S^2\,,\, \ldots\,,\, S^{\nu-1}.$$

In der That sind die Terme der letzten Reihe von einander ver-

schieden, wenn ν die kleinste Zahl ist, für welche man $S^{\nu} = 1$ hat; denn wenn $S^{\mu'+\nu'} = S^{\mu'}$ wäre, so müsste $S^{\nu'} = 1$ sein, was unmöglich ist, da $\nu' < \nu$ sein soll.

Den kleinsten der Exponenten ν, für welche $S^{\nu} = 1$ ist, nennt man die Ordnung der Substitution S. Mit andern Worten ist die Ordnung einer Substitution die Zahl, welche angiebt, wie oft man die Substitution auf eine Permutation anwenden muss, um eben dieselbe Permutation wieder zu erhalten. Wie man sieht, sind S^{ν}, $S^{2\nu}$, $S^{3\nu}$, ... die einzigen Potenzen von S, welche sich auf die Einheit reduciren.

Wir wollen die Formel $S^{\nu q+r} = S^{r}$ auf die negativen Werthe von r ausdehnen. Schreibt man $-r$ statt r, so folgt

$$S^{\nu q-r} = S^{-r},$$

und diese Formel definirt die negativen Potenzen einer Substitution S, vorausgesetzt, dass die Zahl q so gewählt wird, dass $\nu q - r$ positiv ist. Setzt man im Besonderen $r = 1$, so kann man $q = 1$ annehmen, und erhält

$$S^{\nu-1} = S^{-1}.$$

Das Produkt der Substitutionen S und S^{-1} ist die Einheit; man nennt die eine dieser Substitutionen die Umkehrung der andern. Hat man

$$S = \begin{pmatrix} A_1 \\ A_0 \end{pmatrix},$$

so ist offenbar

$$S^{-1} = \begin{pmatrix} A_0 \\ A_1 \end{pmatrix}.$$

Wenn eine Substitution S von der Ordnung ν ist, so ist die μ^{te} Potenz von S von der Ordnung $\frac{\nu}{\vartheta}$, worin ϑ den grössten gemeinschaftlichen Divisor der Zahlen μ und ν bezeichnet. Damit man nämlich $(S^{\mu})^{x} = 1$ oder $S^{\mu x} = 1$ habe, muss μx durch ν oder x durch $\frac{\nu}{\vartheta}$ theilbar sein; diese Gleichheit besteht zudem wenn $x = \frac{\nu}{\vartheta}$ angenommen wird. Folglich stellt der Quotient $\frac{\nu}{\vartheta}$ die Ordnung von S^{μ} dar.

Wenn im Besonderen μ und ν relative Primzahlen sind, so ist S^{μ} von der Ordnung ν. Setzt man in diesem Falle

$$S^\mu = T,$$

so ist die Substitution S in der Reihe der Potenzen von T enthalten. Wird nämlich die vorstehende Gleichung auf die x^{te} Potenz erhoben, so ergiebt sich

$$S^{\mu x} = T^x \quad \text{oder} \quad S^{\mu x - \nu y} = T^x,$$

worin y irgend eine ganze Zahl bezeichnet. Da aber ν und μ prim zu einander sind, so kann man es stets so einrichten, dass die ganzen Zahlen x, y der Gleichung $\mu x - \nu y = 1$ genügen, und dann ist

$$S = T^x.$$

Cyclische Substitutionen.

395. Es sei

$$A_0 = abc \ldots kl$$

eine der Permutationen der n Buchstaben $a, b, c, \ldots, k, l$. Schreibt man den Buchstaben a, welcher in A_0 den ersten Platz einnimmt, rechts neben den letzten Buchstaben l, so erhält man die neue Permutation

$$A_1 = bc \ldots kla,$$

und die Substitution, durch welche man von A_0 zu A_1 übergeht, ist

$$\binom{A_1}{A_0} = \binom{bc \ldots kla}{abc \ldots kl}.$$

Diese Substitution lässt sich in folgender Weise ausführen: Man theilt den Umfang eines Kreises in n gleiche Theile und schreibt an die Theilpunkte der Reihe nach die Buchstaben der Permutation A_0; dreht man sodann den Kreis in geeigneter Richtung um einen Winkel, welcher gleich dem n^{ten} Theile von $4R$ ist, und ersetzt jeden Buchstaben durch denjenigen, welcher in Folge dieser Drehung an den Platz des ersteren kommt, so erhält man die Permutation A_1. Aus diesem Grunde heisst die in Rede stehende Substitution eine *cyclische*.

Die *Ordnung einer cyclischen Substitution ist offenbar gleich der Anzahl n der Buchstaben, welche sie auf andere Plätze bringt.* Jedesmal nämlich, wo der angegebene Kreis sich um den n^{ten} Theil von $4R$ dreht, wird

die Substitution einmal vollzogen. Um nun zur Permutation zu gelangen, von der man ausging, muss der Kreis immer in demselben Sinne sich $n$mal um den n^{ten} Theil von $4R$ drehen, d. h. die Substitution muss $n$mal vollführt werden; die Ordnung der Substitution ist daher gleich n.

Gewöhnlich stellt man eine cyclische Substitution durch irgend eine (in Parenthesen gesetzte) Permutation dar, deren Buchstaben so geordnet sind, dass jeder in Folge der Substitution den vorhergehenden ersetzt. Man hat auf diese Weise

$$\begin{pmatrix} bc \ldots kla \\ abc \ldots kl \end{pmatrix} = (a, b, c, \ldots, k, l) = (b, c, \ldots, k, l, a), \ldots .$$

Zerlegung einer Substitution in Cyclen.

396. Lehrsatz I. — Jede Substitution, die nicht selbst cyclisch ist, ist das Product mehrerer auf verschiedene Buchstaben bezüglichen cyclischen Substitutionen.

Es sei S eine beliebige Substitution, und a einer der Buchstaben, der seinen Platz verlieren und durch einen Buchstaben b ersetzt werden soll; b selbst wird durch einen dritten Buchstaben c ersetzt werden, u. s. w.; auf diese Weise wird man schliesslich zu einem Buchstaben f gelangen müssen, welcher durch a zu ersetzen ist. Die bisher berücksichtigten Buchstaben haben offenbar die cyclische Substitution $(a, b, c, \ldots, f)$ erlitten. Nimmt man weiter einen der übrigen Buchstaben und wiederholt das eben dargelegte Verfahren, so erhält man eine neue Gruppe von Buchstaben, mit welchen eine cyclische Substitution zu vollziehen ist. Auf diese Weise kann man fortfahren, bis alle Buchstaben erschöpft sind, die in Folge der Substitution andere Plätze einnehmen.

Bezeichnen $C_0, C_1, C_2, \ldots$ die verschiedenen cyclischen Substitutionen, die das vorstehende Verfahren geliefert hat, so ist

$$S = C_0 C_1 C_2 \ldots,$$

und diese Formel drückt den Werth von S als Produkt cyclischer Factoren aus. Diese Factoren heissen die Cyclen der Substitution S. Diejenigen Cyclen, welche nur zwei Buchstaben enthalten, werden Transpositionen genannt (No. 235).

Betrachten wir z. B. die Substitution

$$S = \begin{pmatrix} h\,k\,d\,f\,b\,j\,a\,g\,e\,c\,i \\ a\,b\,c\,d\,e\,f\,g\,h\,i\,j\,k \end{pmatrix},$$

so ergiebt sich auf dem eben dargelegten Wege

$$S = (a\,,h\,,g)\;(b\,,k\,,i\,,e)\;(c\,,d\,,f\,,j).$$

Wenn eine Substitution einige Buchstaben des betrachteten Systems nicht versetzt, so kommen diese Buchstaben in dem einfachsten Ausdrucke von S nicht vor, und ebenso wenig sind sie in den cyclischen Factoren enthalten, deren Produkt S ist. Man kann ihr Vorhandensein, wenn man will, dadurch ausdrücken, dass man in S Cyclen einführt, die aus je einem dieser Buchstaben bestehen, und die offenbar identische Substitutionen darstellen. So lässt sich im Falle eines Systems von sechs Buchstaben $a\,,b\,,c\,,d\,,e\,,f$ die Substitution

$$S = \begin{pmatrix} d\;c\;b\;a\;e\;f \\ a\;b\;c\;d\;e\;f \end{pmatrix}$$

folgendermassen schreiben:

$$S = (a\,,d)\;(b\,,c)\;(e)\;(f).$$

397. Lehrsatz II. — Die Ordnung einer Substitution ist gleich dem kleinsten gemeinschaftlichen Vielfachen der Zahlen, welche die Ordnungen der Cyclen der Substitution ausdrücken.

Es sei

$$S = C_0\;C_1\;C_2\;\ldots$$

die in cyclische Factoren zerlegte Substitution S. Bezeichnet ν die Ordnung von S, so hat man

$$S^\nu = 1\,,$$

oder, da es offenbar gestattet ist, die Reihenfolge der Factoren von S^ν zu ändern,

$$C_0^\nu\;C_1^\nu\;C_2^\nu\;\ldots = 1\,.$$

Damit die letzte Formel bestehe, ist erforderlich und hinreichend, dass

$$C_0^\nu = 1\,,\; C_1^\nu = 1\,,\; C_2^\nu = 1\,,\;\ldots$$

sei. Bezeichnet nun α_0 die Ordnung von C_0, so reduciren sich nur diejenigen Potenzen von C_0 auf 1, welche die Exponenten $\alpha_0\,,\,2\alpha_0\,,\,3\alpha_0\,,\,\ldots$ haben; folglich ist ν ein Vielfaches von α_0.

Ebenso sieht man, dass ν durch jede der Zahlen $\alpha_1, \alpha_2, \ldots$ theilbar sein muss, welche beziehungsweise die Ordnungen der Cyclen $C_1, C_2, \ldots$ ausdrücken, und da die Zahl ν die Ordnung von S bezeichnet, so muss sie gleich dem kleinsten gemeinschaftlichen Vielfachen der Zahlen $\alpha_0, \alpha_1, \alpha_2, \ldots$ sein.

398. Eine Substitution heisst regelmässig, wenn sie cyclisch oder aus cyclischen Factoren von ein und derselben Ordnung zusammengesetzt ist. Jede andere Substitution wird eine unregelmässige genannt.

Lehrsatz III. — Die μ^{te} Potenz einer cyclischen Substitution ν^{ter} Ordnung S ist selbst cyclisch, wenn μ prim zu ν ist. Wenn aber die Zahlen μ und ν einen grössten gemeinschaftlichen Divisor $\vartheta > 1$ haben, so ist S^μ eine regelmässige Substitution, die aus ϑ Cyclen von der Ordnung $\frac{\nu}{\vartheta}$ besteht.

Wir stellen wieder die ν Buchstaben der cyclischen Substitution S an die Theilpunkte einer in ν gleiche Theile getheilten Kreisperipherie. Durch die Substitution S^μ wird jeder Buchstabe durch denjenigen ersetzt, dessen Entfernung von jenem μmal so gross als der ν^{te} Theil der Peripherie ist. Geht man also von irgend einem Theilpunkte aus immer in demselben Sinne weiter, bis man zum Ausgangspunkte zurückgelangt, und betrachtet dabei nur den 1ten, μ^{ten}, $2\mu^{\text{ten}}$, $3\mu^{\text{ten}}$, u. s. w. Theilpunkt, so erleiden die an diese Punkte gestellten Buchstaben in Folge der Substitution S^μ eine cyclische Versetzung. Nun muss die Anzahl x dieser Buchstaben von der Beschaffenheit sein, dass das Produkt von $\mu \cdot \frac{2\pi}{\nu}$ in x das kleinstmögliche Vielfache von 2π ist; mit andern Worten, μx muss die kleinste der Zahlen sein, in welche ν aufgeht. Bezeichnet daher ϑ den grössten gemeinschaftlichen Divisor der Zahlen μ und ν, so hat man $x = \frac{\nu}{\vartheta}$. Daraus geht hervor, dass S^μ das Produkt von ϑ cyclischen Substitutionen ist, von denen jede $\frac{\nu}{\vartheta}$ Buchstaben enthält. Wenn μ und ν relative Primzahlen sind, so ist $\vartheta = 1$ und die Substitution S^μ cyclisch.

Beispiel. — Wir betrachten die cyclische Substitution 6ter Ordnung

$$S = (a, b, c, d, e, f).$$

Die Potenzen derselben sind

$$S = (a, b, c, d, e, f),$$
$$S^2 = (a, c, e)(b, d, f),$$
$$S^3 = (a, d)(b, e)(c, f),$$
$$S^4 = (a, e, c)(b, f, d),$$
$$S^5 = (a, f, e, d, c, b),$$
$$S^6 = 1.$$

399. Lehrsatz IV. — Umgekehrt ist jede regelmässige Substitution eine Potenz einer cyclischen Substitution.

Die aus ϑ Cyclen von der Ordnung $\frac{\nu}{\vartheta}$ bestehende regelmässige Substitution sei

$$S = (a_1, b_1, \ldots, g_1)(a_2, b_2, \ldots, g_2) \ldots (a_\vartheta, b_\vartheta, \ldots, g_\vartheta).$$

Macht man

$$C = (a_1, a_2, \ldots, a_\vartheta, b_1, b_2, \ldots, b_\vartheta, \ldots, g_1, g_2, \ldots, g_\vartheta),$$

so ist offenbar

$$S = C^\vartheta.$$

Zerlegung einer gegebenen Substitution in primitive Factoren.

400. Die Eigenschaften, die wir in diesem Kapitel noch zu erörtern haben, sind meist von Cauchy entdeckt, der sie im 3. Bande seiner Exercices d'Analyse et de Physique mathématique veröffentlicht hat.

Es sei S irgend eine der Substitutionen, die man aus n Buchstaben bilden kann. Wir zerlegen die Ordnung ν von S in Primfactoren; es ergebe sich

$$\nu = \alpha\beta\gamma \ldots,$$

wo $\alpha, \beta, \gamma, \ldots$ Potenzen ungleicher Primzahlen darstellen. Ferner bezeichne ν' den Quotienten der Division von ν durch α, d. h. das Produkt $\beta\gamma\ldots$, und μ irgend eine positive oder negative ganze Zahl. Da α und ν' relative Primzahlen sind, so lassen sich zwei positive oder negative ganze Zahlen x und μ' von der Beschaffenheit ermitteln, dass

$$\mu = \nu' x + \alpha \mu' \text{ oder } \frac{\mu}{\nu} = \frac{x}{\alpha} + \frac{\mu'}{\nu'}$$

ist. Bezeichnet weiter ν'' den Quotienten der Division von ν' durch β, so kann man zwei ganze Zahlen y und μ'' finden, für welche man

$$\mu' = \nu'' y + \beta \mu'' \text{ oder } \frac{\mu'}{\nu'} = \frac{y}{\beta} + \frac{\mu''}{\nu''},$$

folglich

$$\frac{\mu}{\nu} = \frac{x}{\alpha} + \frac{y}{\beta} + \frac{\mu''}{\nu''}$$

hat, und es liegt auf der Hand, dass man $\mu'' = 0$ machen kann, wenn $\nu'' = 1$ ist. Auf diese Weise bringt man den Bruch $\frac{\mu}{\nu}$ auf die Form

$$\frac{\mu}{\nu} = \frac{x}{\alpha} + \frac{y}{\beta} + \frac{z}{\gamma} + \ldots;$$

darin stellen $x, y, z, \ldots$ ganze Zahlen dar. Diese Formel, die für jeden Werth von μ besteht, liefert für $\mu = 1$

$$1 = \frac{\nu}{\alpha} x + \frac{\nu}{\beta} y + \frac{\nu}{\gamma} z + \ldots.$$

Danach lässt sich die gegebene Substitution S in folgender Weise schreiben:

$$S = S^{\frac{\nu}{\alpha} x + \frac{\nu}{\beta} y + \frac{\nu}{\gamma} z + \ldots} = S^{\frac{\nu}{\alpha} x} S^{\frac{\nu}{\beta} y} S^{\frac{\nu}{\gamma} z} \ldots,$$

und wenn der Kürze wegen

$$S^{\frac{\nu}{\alpha}} = P,\ S^{\frac{\nu}{\beta}} = Q,\ S^{\frac{\nu}{\gamma}} = R, \ldots$$

gesetzt wird, so ist

$$S = P^x Q^y R^z \ldots.$$

Da die Substitution S von der Ordnung ν ist, so muss P von der Ordnung α, Q von der Ordnung β, R von der Ordnung γ, u. s. w. sein. Ausserdem sind die Zahlen $x, y, z, \ldots$ beziehungsweise prim zu $\alpha, \beta, \gamma, \ldots$; folglich sind $P^x, Q^y, R^z, \ldots$ beziehungsweise von den Ordnungen $\alpha, \beta, \gamma, \ldots$. Die vorstehende Formel zerlegt S in Factoren, deren Ordnungen beziehungsweise die Potenzen der Primzahlen sind, welche zum Produkt die Ordnung von S haben, und da diese Factoren sämmtlich Potenzen der Substitution S sind, so kann man sie offenbar in beliebiger Reihenfolge schreiben.

Eine Substitution heisst **primitiv**, wenn ihre Ordnung eine Primzahl oder eine Potenz einer Primzahl ist. Wenn eine primitive Substitution von der Ordnung $\alpha = p^\lambda$ ist, worin p eine Primzahl bedeutet, so muss die Ordnung irgend eines ihrer cyclischen Factoren ein Divisor von p^λ, also eine der Zahlen $1, p, p^2, \ldots, p^{\lambda-1}$ sein. Aus dem Vorhergehenden ist ersichtlich, dass jede Substitution als Produkt gegen einander vertauschbarer primitiven Substitutionen dargestellt werden kann.

Beispiel. — Die Ordnung der cyclischen Substitution

$$S = (a, b, c, d, e, f)$$

ist 2×3. Man hat

$$S = S^3 . \; S^{-2} = S^3 . \; S^4,$$

so dass S^3 und S^4 die primitiven Substitutionen sind, deren Produkt S ist. Nach dem Früheren ist

$$S^3 = (a, d)(b, e)(c, f),$$
$$S^4 = (a, e, c)(b, f, d).$$

Ähnliche Substitutionen.

401. Zwei Substitutionen heissen **ähnlich**, wenn sie dieselbe Anzahl von cyclischen Factoren und dieselbe Anzahl von Buchstaben in den entsprechenden Cyclen enthalten.

Danach sind zwei cyclische Substitutionen derselben Ordnung einander ähnlich; zwei regelmässige Substitutionen derselben Ordnung sind ähnlich, wenn sie aus gleich viel cyclischen Factoren bestehen.

Lehrsatz. — Wenn S und S' zwei ähnliche Substitutionen bezeichnen, so giebt es eine Substitution P von der Beschaffenheit, dass

$$S'P = PS \text{ oder } S' = PSP^{-1}$$

ist. Wenn umgekehrt eine Substitution P existirt, für welche die vorstehende Formel stattfindet, so sind S und S' ähnliche Substitutionen.

Es sei

$$S = \binom{B}{A},$$

wo A und B zwei Permutationen der n Buchstaben $a, b, c, \ldots, k, l$ bezeichnen. Wir nehmen an, dass $a', b', c', \ldots, k', l'$ die-

selben Buchstaben, in irgend einer andern Reihenfolge geschrieben, darstellen und bezeichnen mit A' und B' das, was beziehungsweise aus A und B wird, wenn man die Buchstaben accentuirt. Jede Substitution S', welche S ähnlich ist, kann offenbar durch

$$S' = \binom{B'}{A'}$$

dargestellt werden. Bezeichnet ausserdem P die Substitution, deren Wirkung die Accentuation der Buchstaben ist, so hat man

$$P = \binom{A'}{A} = \binom{B'}{B} \text{ und } P^{-1} = \binom{A}{A'} = \binom{B}{B'}.$$

Daraus ergiebt sich

$$PSP^{-1} = \binom{B'}{B}\binom{B}{A}\binom{A}{A'}.$$

Die Substitution $\binom{A}{A'}$ muss zuerst ausgeführt werden; sie ersetzt die Buchstaben von A' durch diejenigen von A. Die zweite Substitution ersetzt sodann A durch B, endlich die dritte B durch B'. Man hat daher

$$PSP^{-1} = \binom{B'}{A'} \text{ oder } S' = PSP^{-1},$$

und wenn beiderseits zur Rechten mit P multiplicirt wird,

$$S'P = PS.$$

Wenn umgekehrt die letzte Formel besteht, so sind S und S' ähnliche Substitutionen. Man hat nämlich der Voraussetzung nach, wenn die Substitution S wieder durch $\binom{B}{A}$ und die Substitution P durch $\binom{A'}{A}$ oder $\binom{B'}{B}$ dargestellt wird,

$$S' = PSP^{-1}$$

oder

$$S' = \binom{B'}{B}\binom{B}{A}\binom{A}{A'} = \binom{B'}{A'};$$

mithin ist S' der Substitution S ähnlich.

Zusatz I. — Die der Substitution S ähnliche Substitution PSP^{-1} wird dadurch erhalten, dass man die Substitution P in den Cyclen von S ausführt.

Es liegt nämlich auf der Hand, dass diese Operation gleichbedeutend ist mit der Accentuation der Buchstaben, die wir im vorhergehenden Beweise in Anwendung gebracht haben.

Zusatz II. — Die Produkte ST und TS, welche durch Multiplication von zwei beliebigen Substitutionen S und T erhalten werden, sind ähnliche Substitutionen. Es sei nämlich

$$ST = P \; , \; TS = Q \; .$$

Multiplicirt man die erste dieser Gleichungen zur Rechten mit T^{-1}, so folgt

$$S = PT^{-1} \, ,$$

und wenn dieser Werth von S in die zweite der vorstehenden Formeln eingesetzt wird, so ergiebt sich

$$Q = TPT^{-1} \, .$$

Diese Relation zeigt, dass P und Q ähnliche Substitutionen sind.

Beispiel. — Wir setzen die Anzahl der Buchstaben gleich 6 voraus und machen

$$S = (a\,,\,b\,,\,c\,,\,d)\,(e\,,\,f) \;,\; T = (a\,,\,b\,,\,c)\,(d\,,\,e\,,\,f)\,;$$

dann ergeben sich die beiden ähnlichen Substitutionen 5ter Ordnung:

$$ST = (a\,,\,c\,,\,b\,,\,d\,,\,f)\,(e) \;,\; TS = (a\,,\,c\,,\,e\,,\,d\,,\,b)\,(f) \, .$$

Über die Anzahl der Substitutionen, welche einer gegebenen Substitution ähnlich sind.

402. Die Anzahl der Buchstaben, die man betrachtet, werde durch n dargestellt, und es sei S eine Substitution, welche m_1 Cyclen von der Ordnung n_1, m_2 Cyclen von der Ordnung $n_2, \ldots,$ endlich m_ω Cyclen von der Ordnung n_ω enthält; dann ist

$$n = m_1\,n_1 + m_2\,n_2 + \cdots + m_\omega\,n_\omega\,;$$

darin kann jede der Zahlen $n_1 \, , \, n_2 \, , \ldots , \, n_\omega$ sich auf die Einheit reduciren.

Wir wollen zunächst die Anzahl der verschiedenen Formen ermitteln, welche man der in cyclische Factoren zerlegten Substitution S beilegen kann, ohne die Parenthesen zu versetzen, welche jeden Cyclus einschliessen, und ohne folglich die Anzahl der in einem cyclischen Factor von bestimmtem Range enthaltenen Buchstaben zu verändern. Die einzigen Veränderungen, die man danach noch vornehmen kann, ohne S zu ändern, bestehen darin, dass man die cyclischen Factoren ein und derselben Ord-

nung unter einander vertauscht, oder dass man der Reihe nach in jedem cyclischen Factor irgend einem der darin enthaltenen Buchstaben den ersten Platz anweist. Daraus ergiebt sich, dass die Anzahl M der verschiedenen Formen, welche man S beilegen kann, folgende ist:

$$M = (1 \,.\, 2 \ldots m_1)\,(1 \,.\, 2 \ldots m_2) \ldots (1 \,.\, 2 \ldots m_\omega)\, n_1^{m_1}\, n_2^{m_2} \ldots n_\omega^{m_\omega}\,.$$

Es sei jetzt $\mathfrak{N}$ die Anzahl der verschiedenen Substitutionen $S, S', S'', \ldots$, welche S ähnlich sind. Schreibt man der Reihe nach jede dieser Substitutionen unter die M verschiedenen Formen, die man ihr beilegen kann, ohne die Parenthesen zu versetzen, und unterdrückt sodann die Parenthesen, so erhält man $M\mathfrak{N}$ Permutationen. Offenbar ist aber bei diesem Verfahren keine Permutation der n Buchstaben ausgelassen worden, und man hat daher

$$M\mathfrak{N} = 1 \,.\, 2 \,.\, 3 \ldots n = N,$$

folglich

$$\mathfrak{N} = \frac{N}{M}\,.$$

Gegen einander vertauschbare Substitutionen.

403. Zwei Substitutionen, welche sich auf Potenzen ein und derselben Substitution reduciren, sind gegen einander vertauschbar; dasselbe ist offenbar mit zwei Substitutionen der Fall, welche keinen Buchstaben gemeinschaftlich haben. Es ist aber von grosser Wichtigkeit, allgemein die Bedingung kennen zu lernen, welcher zwei Substitutionen genügen müssen, damit sie sich gegen einander vertauschen lassen. Diese Frage wollen wir jetzt in Angriff nehmen.

Es seien S und T zwei Substitutionen, die wir als gegen einander vertauschbar voraussetzen; dann ist

$$ST = TS \text{ oder } S = TST^{-1}.$$

Wir haben gesehen, dass die Substitution TST^{-1} sich aus S dadurch ergiebt, dass man die Substitution T in den Cyclen von S ausführt. Damit also die Substitutionen S und T gegen einander vertauschbar seien, ist erforderlich und hinreichend, dass die Substitution S unverändert bleibt, wenn die Buchstaben ihrer Cyclen der Substitution T unterworfen werden. Folglich kann der Einfluss der Substitution T auf S nur in der Vertauschung der Cyclen

ein und derselben Ordnung und in der Versetzung bestehen, welche es gestattet, in einem Cyclus irgend einen Buchstaben auf den ersten Platz zu bringen, ohne die cyclische Aufeinanderfolge der Buchstaben dieses Cyclus zu ändern. Jede der erwähnten Vertauschungen der Cyclen ein und derselben Ordnung ist entweder selbst cyclisch, oder gleichbedeutend mit mehreren an verschiedenen Cyclen gleichzeitig vollführten cyclischen Vertauschungen. Es seien (C_o), (C_1), ..., $(C_{\mu-1})$ Cyclen derselben Ordnung, welche eine solche cyclische Vertauschung zu erleiden haben. Die Substitution T kann ferner, wie wir soeben bemerkten, die Versetzung zur Folge haben, welche es gestattet, in jedem dieser Cyclen irgend einen Buchstaben auf den ersten Platz zu bringen. Da aber die Gruppirung C_o, durch welche der Cyclus (C_o) gebildet wird, nach Belieben gewählt worden ist, so kann man, um den Cyclus (C_1) zu bilden, immer die Gruppirung C_1 nehmen, welche die Substitution T an die Stelle von C_o setzen soll. Ebenso kann man, um die folgenden Cyclen (C_2), ..., $(C_{\mu-1})$ zu bilden, die Gruppirungen C_2, ..., $C_{\mu-1}$ nehmen, welche beziehungsweise an die Plätze von C_1, C_2, ..., $C_{\mu-2}$ treten. Die letzte Gruppirung $C_{\mu-1}$ wird im Allgemeinen nicht durch C_o, sondern durch eine andere Gruppirung C'_o ersetzt werden, welche so beschaffen ist, dass die Cyclen (C_o) und (C'_o) identisch sind. Setzt man somit

$$P = (C_o)(C_1)\ldots(C_{\mu-1}),\ Q = \begin{pmatrix} C_1\, C_2 \ldots C_{\mu-1}\, C'_o \\ C_o\, C_1 \ldots C_{\mu-2}\, C_{\mu-1} \end{pmatrix}$$

und bezeichnet mit P' und Q', P'' und Q'', ... Substitutionen, welche P und Q analog sind, sich aber auf verschiedene Buchstaben beziehen, so ergiebt sich nothwendig

$$S = PP'P'' \ldots,\ T = QQ'Q'' \ldots;$$

darin sind P und Q, P' und Q', P'' und Q'', ... Paare von vertauschbaren Substitutionen, deren Anzahl sich auf Eins reduciren kann.

404. Wir sind auf diese Weise zur Betrachtung der beiden Substitutionen P und Q geführt. Die erste derselben ist regelmässig, und wir werden sehen, dass dieselbe Eigenschaft auch der zweiten zukommt.

Es sei i die Ordnung der Cyclen von P. Der grösseren Klarheit wegen werden wir in der Folge die in ein und demselben

Cyclus enthaltenen Buchstaben durch ein und dasselbe, mit den Indices $0, 1, 2, \ldots, (i-1)$ versehene Zeichen ausdrücken. Wir setzen also

$$C_0 = a_0\, a_1\, a_2\, a_3 \ldots a_{i-1},$$
$$C_1 = b_0\, b_1\, b_2\, b_3 \ldots b_{i-1},$$
$$\ldots\ldots\ldots\ldots\ldots,$$
$$C_{\mu-2} = e_0\, e_1\, e_2\, e_3 \ldots e_{i-1},$$
$$C_{\mu-1} = f_0\, f_1\, f_2\, f_3 \ldots f_{i-1},$$

und treffen ausserdem die Uebereinkunft, dass jedes der Zeichen $a, b, \ldots, e, f$, welches den Index $iq + \alpha$ hat, denselben Buchstaben bezeichnen soll, wie wenn sein Index auf den Rest α der Division von $iq + \alpha$ durch i reducirt wäre. Demgemäss können wir

$$C'_0 = a_\varrho\, a_{\varrho+1}\, a_{\varrho+2} \ldots a_{\varrho+i-1}$$

setzen. Wenn die Zahl ϱ Null ist, so hat man $C'_0 = C_0$, und wird dann

$$(G_\xi) = (a_\xi, b_\xi, c_\xi, \ldots, e_\xi, f_\xi)$$

gesetzt, so ist offenbar

$$Q = (G_0)\,(G_1)\,(G_2) \ldots (G_{i-1}).$$

Wir nehmen aber an, ϱ sei von Null verschieden. Wie in dem eben untersuchten Falle wird durch die Substitution Q jeder der $\mu - 1$ ersten Buchstaben der Gruppirung

$$a_\xi\, b_\xi\, c_\xi \ldots e_\xi\, f_\xi$$

durch den folgenden ersetzt; der letzte Buchstabe f_ξ wird durch $a_{\xi+\varrho}$ ersetzt; ferner wird jeder der $\mu - 1$ ersten Buchstaben der Gruppirung

$$a_{\xi+\varrho}\, b_{\xi+\varrho} \ldots e_{\xi+\varrho}\, f_{\xi+\varrho}$$

durch den folgenden, der Buchstabe $f_{\xi+\varrho}$ durch $a_{\xi+2\varrho}$ ersetzt, u. s. w. Der Kreis wird sich jedenfalls schliessen; dies kann aber nur dann geschehen, wenn man zum Buchstaben $f_{\xi+(\lambda-1)\varrho}$ gelangt ist, dessen Index die Beschaffenheit hat, dass $\lambda\varrho$ durch i theilbar ist. Daraus ist ersichtlich, dass man einen Cyclus von Q erhält, wenn man die λ Gruppirungen

$$a_\xi\, b_\xi \ldots f_\xi ,$$
$$a_{\xi+\varrho}\, b_{\xi+\varrho} \ldots f_{\xi+\varrho} ,$$
$$\ldots\ldots\ldots\ldots ,$$
$$a_{\xi+(\lambda-1)\varrho}\, b_{\xi+(\lambda-1)\varrho} \ldots f_{\xi+(\lambda-1)\varrho}$$

neben einander schreibt, und wenn dieser Cyclus durch (G_ξ) bezeichnet wird, so ist offenbar

$$Q = (G_0)\,(G_1)\,(G_2) \ldots (G_{\varrho-1}) .$$

Die Anzahl j der in jedem Cyclus (G) enthaltenen Buchstaben ist

$$j = \lambda\mu ,$$

und da ϱ Cyclen (G) vorhanden sind, so ist die Gesammtzahl $i\mu$ der Buchstaben gleich $\lambda\mu\varrho$, also

$$i = \lambda\varrho .$$

Aus der vorstehenden Betrachtung ergiebt sich eine sehr einfache Regel, die Ausdrücke der beiden gegen einander vertauschbaren Substitutionen P und Q zu bestimmen. Wir bilden die Tabelle

$$a_\xi ,\ a_{\xi+1} , \ldots ,\ a_{\xi+\varrho-1} ,$$
$$b_\xi ,\ b_{\xi+1} , \ldots ,\ b_{\xi+\varrho-1} ,$$
$$\ldots\ldots\ldots\ldots ,$$
$$e_\xi ,\ e_{\xi+1} , \ldots ,\ e_{\xi+\varrho-1} ,$$
$$f_\xi ,\ f_{\xi+1} , \ldots ,\ f_{\xi+\varrho-1} ,$$

welche aus μ Horizontalreihen und aus ϱ Verticalreihen besteht. Die aus den Horizontalreihen gebildeten Gruppirungen bezeichnen wir mit

$$\mathfrak{A}_\xi ,\ \mathfrak{B}_\xi , \ldots ,\ \mathfrak{E}_\xi ,\ \mathfrak{F}_\xi ,$$

die aus den Verticalreihen gebildeten mit

$$\mathfrak{M}_\xi ,\ \mathfrak{M}_{\xi+1} , \ldots ,\ \mathfrak{M}_{\xi+\varrho-1} ;$$

dann ergeben sich folgende Ausdrücke für die Cyclen von P und von Q:

$$C_0 = \mathfrak{A}_0\, \mathfrak{A}_\varrho\, \mathfrak{A}_{2\varrho} \ldots \mathfrak{A}_{(\lambda-1)\varrho} ,$$
$$C_1 = \mathfrak{B}_0\, \mathfrak{B}_\varrho\, \mathfrak{B}_{2\varrho} \ldots \mathfrak{B}_{(\lambda-1)\varrho} ,$$
$$\ldots\ldots\ldots\ldots ,$$
$$C_{\mu-2} = \mathfrak{E}_0\, \mathfrak{E}_\varrho\, \mathfrak{E}_{2\varrho} \ldots \mathfrak{E}_{(\lambda-1)\varrho} ,$$
$$C_{\mu-1} = \mathfrak{F}_0\, \mathfrak{F}_\varrho\, \mathfrak{F}_{2\varrho} \ldots \mathfrak{F}_{(\lambda-1)\varrho} ,$$

und
$$G_0 = \mathfrak{M}_0\, \mathfrak{M}_\varrho\, \mathfrak{M}_{2\varrho} \ldots \mathfrak{M}_{(\lambda-1)\varrho},$$
$$G_1 = \mathfrak{M}_1\, \mathfrak{M}_{\varrho+1} \ldots \mathfrak{M}_{(\lambda-1)\varrho+1},$$
$$\ldots\ldots\ldots\ldots\ldots,$$
$$G_{\varrho-2} = \mathfrak{M}_{\varrho-2}\, \mathfrak{M}_{2\varrho-2} \ldots \mathfrak{M}_{\lambda\varrho-2},$$
$$G_{\varrho-1} = \mathfrak{M}_{\varrho-1}\, \mathfrak{M}_{2\varrho-1} \ldots \mathfrak{M}_{\lambda\varrho-1}.$$

Wenn $\varrho = i$ ist, so hat man $\lambda = 1$ und $j = \mu$; dieser Fall ist mit dem bereits besonders untersuchten Falle gleichbedeutend, in welchem $\varrho = 0$ ist; wie man sieht, ist er im allgemeinen Falle enthalten.

Aus den vorhergehenden Formeln folgt

$$(C_0)^\varrho = (a_0, a_\varrho, \ldots, a_{(\lambda-1)\varrho})\,(a_1, a_{\varrho+1}, \ldots, a_{(\lambda-1)\varrho+1}) \cdots \times (a_{\varrho-1}, a_{2\varrho-1}, \ldots, a_{\lambda\varrho-1}),$$
$$(C_1)^\varrho = (b_0, b_\varrho, \ldots, b_{(\lambda-1)\varrho})\,(b_1, b_{\varrho+1}, \ldots, b_{(\lambda-1)\varrho+1}) \cdots \times (b_{\varrho-1}, b_{2\varrho-1}, \ldots, b_{\lambda\varrho-1}),$$
$$\ldots\ldots\ldots\ldots\ldots,$$
$$(C_{\mu-1})^\varrho = (f_0, f_\varrho, \ldots, f_{(\lambda-1)\varrho})\,(f_1, f_{\varrho+1}, \ldots, f_{(\lambda-1)\varrho+1}) \cdots \times (f_{\varrho-1}, f_{2\varrho-1}, \ldots f_{\lambda\varrho-1}),$$

und

$$(G_0)^\mu = (a_0, a_\varrho, \ldots, a_{(\lambda-1)\varrho})\,(b_0, b_\varrho, \ldots, b_{(\lambda-1)\varrho}) \cdots \times (f_0, f_\varrho, \ldots, f_{(\lambda-1)\varrho}),$$
$$(G_1)^\mu = (a_1, a_{\varrho+1}, \ldots, a_{(\lambda-1)\varrho+1})\,(b_1, b_{\varrho+1}, \ldots, b_{(\lambda-1)\varrho+1}) \cdots \times (f_1, f_{\varrho+1}, \ldots, f_{(\lambda-1)\varrho+1}),$$
$$\ldots\ldots\ldots\ldots\ldots,$$
$$(G_{\varrho-1})^\mu = (a_{\varrho-1}, a_{2\varrho-1}, \ldots, a_{\lambda\varrho-1}) \cdots\cdots \times (f_{\varrho-1}, f_{2\varrho-1}, \ldots, f_{\lambda\varrho-1}).$$

Daraus ergiebt sich durch Multiplication

$$\left[(C_0)\,(C_1) \ldots (C_{\mu-1})\right]^\varrho = \left[(G_0)\,(G_1) \ldots (G_{\varrho-1})\right]^\mu,$$

d. h.

$$P^\varrho = Q^\mu,$$

und diese beiden gleichen Potenzen von P und von Q sind von Eins verschieden, wofern nicht $\lambda = 1$ ist, denn die Ordnungen der Substitutionen P und Q sind beziehungsweise $\lambda\varrho$ und $\lambda\mu$. Wenn $\lambda = 1$ ist, so können die Substitutionen P und Q keine

Potenz ausser der Einheit gemein haben; denn ein Cyclus von Q und ein Cyclus von P haben nur einen Buchstaben gemeinschaftlich.

405. Die vorstehende Entwicklung, welche uns die Zusammensetzung zweier gegen einander vertauschbaren Substitutionen S und T liefert, muss uns auch die beiden in Nr. 403 erwähnten Fälle vorführen, nämlich den Fall, in welchem die Substitutionen S und T nicht dieselben Buchstaben versetzen, und denjenigen, in welchem S und T Potenzen ein und derselben Substitution sind. Der erstere dieser beiden Fälle tritt ein, wenn die eine der beiden Substitutionen P und Q, P' und Q', P'' und Q'', u. s. w. sich auf Eins reducirt. Damit dies hinsichtlich P und Q der Fall sei, ist erforderlich und hinreichend, dass eine der Zahlen i und j gleich Eins sei. Was den zweiten Fall betrifft, so ist es leicht, folgenden Satz zu begründen:

Damit die Substitutionen P und Q Potenzen ein und derselben Substitution seien, ist erforderlich und hinreichend, dass die Zahlen μ und ϱ keinen gemeinschaftlichen Divisor ausser der Einheit besitzen.

Wir nehmen an, es sei

$$P = R^{\alpha}, \; Q = R^{\beta}. \tag{1}$$

Die Substitution R muss cyclisch sein, denn die Buchstaben $a_{\xi}, a_{\xi+1}, \ldots, a_{\xi+\lambda\varrho-1}$ müssen in ein und demselben Cyclus von R vorkommen, da sie einen Cyclus von R^{α} oder P ausmachen. Ebenso sind die Buchstaben $a_{\zeta}, b_{\zeta}, \ldots, e_{\zeta}, f_{\zeta}$ in ein und demselben Cyclus von R^{β} oder Q enthalten; sie gehören folglich in der Substitution R zu demselben Cyclus, wie die erstgenannten Buchstaben. Dieser Cyclus umfasst daher alle $\lambda\mu\varrho$ Buchstaben, und R ist somit eine cyclische Substitution der Ordnung $\lambda\mu\varrho$. Ausserdem ist R^{α} von der Ordnung $\lambda\varrho$, R^{β} von der Ordnung $\lambda\mu$; folglich sind (Nr. 394) α und β beziehungsweise durch μ und ϱ theilbar. Wenn demnach μ und ϱ einen gemeinschaftlichen Divisor $\delta > 1$ besitzen, so werden auch α und β diesen Divisor zulassen, und wenn

$$\alpha = \delta\alpha', \; \beta = \delta\beta',$$

ferner

$$R' = R^{\delta}$$

gesetzt wird, so erhält man

$$P = R'^{\alpha'} \,, \; Q = R'^{\beta'} \;;$$

diese Formeln können aber nicht stattfinden, da die Substitution R' nicht cyclisch ist. Die Gleichungen (1) erfordern daher, dass μ und ϱ relative Primzahlen seien. Bestimmt man dann zwei ganze Zahlen t und u, welche der Bedingung

$$\varrho t - \mu u = 1$$

genügen, und macht

$$R = Q^t P^{-u} \,,$$

so ergiebt sich

$$P = R^{\mu} \,, \; Q = R^{\varrho} \,.$$

406. Um die vorhergehende Theorie auf ein Beispiel anzuwenden, nehmen wir an, es sei

$$P = (a_0 \,, a_1 \,, a_2 \,, a_3)\,(b_0 \,, b_1 \,, b_2 \,, b_3)\,(c_0 \,, c_1 \,, c_2 \,, c_3) \,,$$
$$Q = (a_0 \,, b_0 \,, c_0 \,, a_2 \,, b_2 \,, c_2)\,(a_1 \,, b_1 \,, c_1 \,, a_3 \,, b_3 \,, c_3).$$

Hier hat man $\lambda = 2$, $\mu = 3$, $\varrho = 2$; da die Zahlen μ und ϱ prim zu einander sind, so sind P und Q Potenzen ein und derselben Substitution. Setzt man

$$R = (a_0 \,, c_3 \,, b_0 \,, a_1 \,, c_0 \,, b_1 \,, a_2 \,, c_1 \,, b_2 \,, a_3 \,, c_2 \,, b_3) \,,$$

so ergiebt sich in der That

$$P = R^3 \,, \; Q = R^2 \,.$$

Macht man dagegen

$$P = (a_0 \,, a_1 \,, a_2 \,, a_3 \,, a_4 \,, a_5)\,(b_0 \,, b_1 \,, b_2 \,, b_3 \,, b_4 \,, b_5) \,,$$
$$Q = (a_0 \,, b_0)\,(a_1 \,, b_1)\,(a_2 \,, b_2)\,(a_3 \,, b_3)\,(a_4 \,, b_4)\,(a_5 \,, b_5) \,,$$

so hat man zwei Substitutionen, die zwar gegeneinander vertauschbar, aber nicht Potenzen einer dritten Substitution sind, da die Zahlen $\mu = 2$ und $\varrho = 6$ den gemeinschaftlichen Divisor 2 besitzen.

Die Substitutionen

$$S = (a \,, b)\,(c \,, d)\,(e \,, f) \,,$$
$$T = (a \,, c)\,(b \,, d)$$

lassen sich gegen einander vertauschen; man hat in diesem Falle

$$S = PP' \,, \; T = QQ' \,,$$

wenn

$$P = (a, b)(c, d), \quad P' = (e, f),$$
$$Q = (a, c)(b, d), \quad Q' = (e)(f)$$

gesetzt wird.

407. Wir wollen jetzt die Anzahl der Substitutionen bestimmen, die gegen eine gegebene Substitution S vertauschbar sind. Bezeichnet T eine Substitution dieser Art, so ist

$$S = TST^{-1},$$

und wir haben gesehen, dass die Substitution TST^{-1} jederzeit dadurch erhalten wird, dass man die Substitution T in den Cyclen von S ausführt. Es giebt also so viele Substitutionen T, welche der vorstehenden Gleichung genügen, als es verschiedene Arten giebt, auf welche man S ausdrücken kann, ohne die Parenthesen zu versetzen, welche die Cyclen umgeben, d. h. ohne die Anzahl der in jedem Cyclus enthaltenen Buchstaben zu ändern. Diese Anzahl ist genau die Zahl, die wir in Nr. 402 durch M dargestellt haben, und als deren Werth sich

$$M = (1.2\ldots m_1)(1.2\ldots m_2)\ldots(1.2\ldots m_\omega)\, n_1^{m_1}\, n_2^{m_2} \ldots n_\omega^{m_\omega}$$

ergab; m_i bezeichnet die Anzahl der in S enthaltenen Cyclen n_i^{ter} Ordnung, und wenn n die Gesammtzahl der Buchstaben ausdrückt, so ist

$$n = m_1 n_1 + m_2 n_2 + \cdots + m_\omega n_\omega.$$

408. Bevor wir die Betrachtung der gegen einander vertauschbaren Substitutionen schliessen, wollen wir zwei wichtige Lehrsätze beweisen, die uns später von Nutzen sein werden.

Lehrsatz I. — Wenn $T, U, V, \ldots, W$ Substitutionen sind, welche gegen eine gegebene Substitution S vertauscht werden können, so ist das aus mehreren der Substitutionen $T, U, \ldots$ gebildete Produkt $TU\ldots$ gleichfalls gegen S vertauschbar.

Man hat nämlich der Voraussetzung nach

$$T = STS^{-1}, \quad U = SUS^{-1}.$$

Daraus ergiebt sich durch Multiplication

$$TU = STS^{-1}\, SUS^{-1}.$$

Im zweiten Gliede dieser Formel können die beiden aufeinander folgenden Factoren S und S^{-1} durch ihr Produkt 1 ersetzt werden; es ist also

$$TU = STUS^{-1} \text{ oder } TU = S \times TU \times S^{-1},$$

woraus hervorgeht, dass das Produkt TU gegen S vertauschbar ist. Hieraus folgert man ohne Weiteres, dass alle Substitutionen von der Form $TUV\ldots$ gegen S vertauschbar sind.

409. Lehrsatz II. — Wenn m eine Zahl bezeichnet, welche prim zur Ordnung einer gegebenen Substitution S ist, so giebt es Substitutionen, welche der Gleichung

(1). $$S^m = TST^{-1}$$

genügen, und zwar ist die Anzahl derselben genau gleich der Anzahl der gegen S vertauschbaren Substitutionen.

Wir bemerken zunächst, dass die Gleichung $S^m = TST^{-1}$ nur dann bestehen kann, wenn m prim zur Ordnung von S ist; denn die Substitutionen TST^{-1} und S sind ähnlich, folglich von derselben Ordnung, und S und S^m können nur dann von derselben Ordnung sein, wenn m prim zur Ordnung von S ist.

Dies vorausgesetzt, sei (C) irgend einer der Cyclen von S und $(\Gamma) = (C)^m$ die m^{te} Potenz dieses Cyclus. Es liegt auf der Hand, dass die Gleichung (1) durch den Werth

$$T = \Theta = \binom{\Gamma}{C}$$

befriedigt wird, worin $\binom{\Gamma}{C}$ der Kürze wegen die Substitution bezeichnet, welche alle Gruppirungen C durch die entsprechenden Gruppirungen Γ ersetzt. In der That wird die Substitution $\Theta S \Theta^{-1}$ dadurch erhalten, dass man alle in den Cyclen von S enthaltenen Gruppirungen C durch die entsprechenden Gruppirungen Γ ersetzt; man hat daher

$$S^m = \Theta S \Theta^{-1}.$$

Danach lässt sich die Gleichung (1) in folgender Weise schreiben:

(2). $$TST^{-1} = \Theta S \Theta^{-1},$$

und wenn beiderseits links mit Θ^{-1}, rechts mit Θ multiplicirt wird, so nimmt (2) die Form an:

(3). $$\Theta^{-1} TST^{-1} \Theta = S.$$

Setzt man endlich

$$T = \Theta U \text{ , also } T^{-1} = U^{-1}\Theta^{-1} ,$$

so reducirt sich (3) auf

$$U S U^{-1} = S ,$$

und diese Formel zeigt, dass U gegen S vertauschbar ist.

Daraus geht hervor, dass man alle Lösungen der Gleichung (1) erhält, wenn man mit einer derselben, Θ, alle gegen S vertauschbaren Substitutionen multiplicirt; die Anzahl der letzteren ist mithin gleich der Anzahl der Substitutionen T.

Beispiel. — Um diesen Satz auf ein Beispiel anzuwenden, nehmen wir wieder die beiden Substitutionen

$$P = (a_0 , a_1 , a_2 , a_3) (b_0 , b_1 , b_2 , b_3) (c_0 , c_1 , c_2 , c_3) ,$$

$$Q = (a_0 , b_0 , c_0 , a_2 , b_2 , c_2) (a_1 , b_1 , c_1 , a_3 , b_3 , c_3) ,$$

die nach dem Früheren Potenzen ein und derselben Substitution sind. Will man aus Q eine Substitution Q' von der Beschaffenheit herleiten, dass

$$P^3 = Q' P Q'^{-1}$$

ist, so genügt es, Q mit der Substitution zu multipliciren, deren beide Terme beziehungsweise die Gruppirungen sind, welche P^3 und P bilden. Man sieht sofort, dass diese Substitution folgende ist:

$$\Theta = (a_1 , a_3) (b_1 , b_3) (c_1 , c_3) ,$$

und man hat

$$Q' = \Theta Q = (a_0 , b_0 , c_0 , a_2 , b_2 , c_2) (a_1 , b_3 , c_1) (a_3 , b_1 , c_3).$$

Reduction einer beliebigen Substitution auf ein Produkt von Transpositionen.

410. Jede Substitution ist mehreren Transpositionen äquivalent. Wenn nämlich in Folge der Substitution S der Buchstabe a einen Platz einnehmen soll, auf welchem jetzt b steht, so ist die Substitution S offenbar gleichbedeutend mit der Transposition (a , b) und einer nur auf die Buchstaben $b , \ldots$ bezüglichen Substitution S', d. h. man hat

$$S = S' \times (a , b).$$

Mit der Substitution S' kann man ebenso verfahren, wie wir mit S verfuhren, und auf diese Weise wird S nach und nach in ein Produkt von Transpositionen zerlegt.

Eine Substitution S lässt sich also dadurch ausführen, dass man mehrere Transpositionen der Reihe nach vollzieht, und zwar kann dies auf mehrere verschiedene Arten geschehen. Welchen Weg man aber auch einschlägt, die Anzahl der Transpositionen, die in Anwendung gebracht werden, ist bis auf ein Viefaches von 2 immer die nämliche. Dies ergiebt sich aus folgendem Satze:

Lehrsatz. — Wenn σ die Anzahl der Cyclen einer auf n Buchstaben bezüglichen Substitution S bezeichnet, so ist das Produkt TS oder ST, welches durch Multiplication der Substitution S und der Transposition T entsteht, eine Substitution, die $\sigma \pm 1$ Cyclen enthält, und zwar ist die Anzahl der Cyclen $\sigma + 1$, wenn die Buchstaben von T verschiedenen Cyclen von S angehören, $\sigma - 1$ im entgegengesetzten Falle.

Es sei

$$T = (a_1 , b_1),$$

und es werde vorausgesetzt, dass die Buchstaben a_1, b_1 zu zwei verschiedenen Cyclen von S gehören, nämlich zu

$$C = (a_1 , a_2 , \ldots , a_i) \;,\; C' = (b_1 , b_2 , \ldots , b_j).$$

Führt man die Substitution S in der Gruppirung

$$a_1 \, a_2 \ldots a_{i-1} \, a_i \, b_1 \, b_2 \ldots b_{j-1} \, b_j$$

aus, so erhält man die neue Gruppirung

$$a_2 \, a_3 \ldots a_i \, a_1 \, b_2 \, b_3 \ldots b_j \, b_1 ,$$

welche in Folge der Transposition T in

$$a_2 \, a_3 \ldots a_i \, b_1 \, b_2 \, b_3 \ldots b_j \, a_1$$

übergeht. Vergleicht man diese Gruppirung mit derjenigen, von der man ausging, so ergiebt sich

$$TCC' = (a_1 , a_2 , \ldots , a_i , b_1 , b_2 , \ldots , b_j).$$

Die Substitution TS enthält daher einen Cyclus weniger als S, und dasselbe gilt von der Substitution ST, welche TS ähnlich ist.

Es mögen jetzt die Buchstaben a_1, b_1 ein und demselben Cyclus

$$C = (a_1 , a_2 , \ldots , a_i , b_1 , b_2 , \ldots , b_j)$$

von S angehören. Wird die Substitution S auf die Gruppirung

$$a_1 \, a_2 \ldots a_{i-1} \, a \;\; b_1 \, b_2 \ldots b_{j-1} \, b_j$$

angewandt, so erhält man

$$a_2\, a_3 \ldots a_i\, b_1\, b_2\, b_3 \ldots b_j\, a_1\,,$$

und wenn man noch die Transposition T vollführt, so folgt

$$a_2\, a_3 \ldots a_i\, a_1\, b_2\, b_3 \ldots b_j\, b_1\,,$$

woraus hervorgeht, dass

$$TC = (a_1\,,\, a_2\,,\, \ldots\,,\, a_i)\,(b_1\,,\, b_2\,,\, \ldots\,,\, b_j)$$

ist. Danach enthält die Substitution TS einen Cyclus mehr als S, und dasselbe ist folglich mit der Substitution ST der Fall.

Anmerkung. — Die Richtigkeit des Satzes setzt offenbar voraus, dass auch die Cyclen mitgezählt werden, welche sich auf einen einzigen Buchstaben reduciren.

Zusatz. — Wenn σ die Anzahl der Cyclen einer aus n Buchstaben gebildeten Substitution S bezeichnet, und wenn diese Substitution dadurch erhalten werden kann, dass man ν gleiche oder ungleiche Transpositionen in einer gewissen Reihenfolge in einander multiplicirt, so ist

$$\nu = (n - \sigma) + 2k\,,$$

wo k eine ganze Zahl bedeutet.

Die erste Transposition kann als eine aus $n - 1$ Cyclen bestehende Substitution angesehen werden, von denen eine von der zweiten Ordnung, die $n - 2$ übrigen von der ersten Ordnung sind. Wird daher diese Transposition mit der zweiten Transposition multiplicirt, so erhält man eine Substitution, die aus $n - 1 \pm 1$ Cyclen gebildet ist. Durch Multiplication dieses ersten Produkts mit der dritten Transposition erhält man ein neues Produkt, in welchem die Anzahl der Cyclen $n - 1 \pm 1 \pm 1$ ist, u. s. w. Hat man also ν Transpositionen in einander multiplicirt, so ist man zur Relation

$$\sigma = n - 1 \pm 1 \pm 1 \pm \ldots \pm 1$$

gelangt, in welcher die Anzahl der zu n addirten positiven oder negativen Einheiten gleich ν ist. Giebt man nun einer der Einheiten, die das Zeichen $+$ haben muss, das Zeichen $-$, so verringert man das zweite Glied unserer Formel um 2 Einheiten. Man hat daher

$$\sigma = n - \nu + 2k \text{ oder } \nu = (n - \sigma) + 2k\,,$$

und folglich ist die Anzahl der Transpositionen, auf welche eine gegebene Substitution S sich reduciren lässt, entweder immer gerade, oder immer ungerade, welchen Weg man auch zur Bildung der Transpositionen einschlagen mag.

411. Das Ergebniss der vorigen Nummer setzt uns in den Stand, die aus n Buchstaben gebildeten $N = 1 . 2 \dots n$ Substitutionen in zwei Klassen zu theilen. Die erste Klasse umfasst die Substitutionen, welche einer geraden Anzahl von Transpositionen äquivalent sind, während die einer ungeraden Anzahl von Transpositionen äquivalenten Substitutionen die zweite Klasse ausmachen.

Es seien

$$1 , S_1 , S_2 , S_3 , \dots$$

die Substitutionen der ersten Art, unter denen sich die Einheit vorfindet, und

$$T_0 , T_1 , T_2 , T_3 , \dots$$

die Substitutionen der zweiten Art. Werden diese Reihen mit einer Transposition (a , b) multiplicirt, so geht die eine offenbar in die andere über; folglich giebt es $\frac{N}{2}$ Substitutionen jeder Art.

Man kann noch die folgenden Resultate aussprechen:

Eine cyclische Substitution ist von der ersten oder von der zweiten Art, jenachdem ihre Ordnung oder die Anzahl ihrer Buchstaben ungerade oder gerade ist.

Das Produkt mehrerer Substitutionen ist von der ersten oder von der zweiten Art, jenachdem die Anzahl der Factoren zweiter Art gerade oder ungerade ist.

Die geraden Potenzen einer jeden Substitution gehören zu den Substitutionen erster Art.

Zweites Kapitel.

Eigenschaften der Systeme conjugirter Substitutionen.

Conjugirte Systeme.

412. Es sind mehrere aus n Buchstaben gebildete Substitutionen gegeben. Wenn man dieselben einmal oder mehrmals mit einander oder mit sich selbst in irgend einer Reihenfolge multiplicirt, und dabei immer nur Substitutionen erhält, die bereits in der Reihe der gegebenen Substitutionen vorkommen, so bilden die letzteren das, was Cauchy ein System conjugirter Substitutionen oder einfach ein conjugirtes System genannt hat. Es leuchtet ein, dass jedes conjugirte System die der Einheit gleiche Substitution enthält.

Unter der Ordnung eines conjugirten Systems versteht man die Anzahl der Substitutionen, welche dasselbe umfasst.

Aus diesen Definitionen geht hervor, dass die $N = 1 . 2 \ldots n$ Substitutionen, welche man aus n Buchstaben bilden kann, ein conjugirtes System N^{ter} Ordnung ausmachen, und dass die Potenzen jeder Substitution ν^{ter} Ordnung ein conjugirtes System ν^{ter} Ordnung bilden.

413. Lehrsatz. — Wenn alle Substitutionen eines conjugirten Systems μ^{ter} Ordnung Γ unter den Substitutionen eines zweiten conjugirten Systems m^{ter} Ordnung G enthalten sind, so ist die Zahl μ ein Divisor von m.

Wir bezeichnen mit

$$(1). \qquad 1 \, , \, S_1 \, , \, S_2 \, , \, S_3 \, , \, \ldots \, , \, S_{\mu-1}$$

die μ Substitutionen des Systems Γ. Diese Substitutionen gehören der Voraussetzung nach zu G, und man hat $m > \mu$. Es sei nun T_1 eine der Substitutionen von G, welche nicht auch dem Sy-

steme Γ, d. h. der Reihe (1) angehören. Multiplicirt man alle Terme dieser Reihe zur Rechten mit T_1, so erhält man die Produkte

(2). $$T_1, S_1 T_1, S_2 T_1, \ldots, S_{\mu-1} T_1,$$

welche sämmtlich unter den Substitutionen des Systems G enthalten sind. Ausserdem sind irgend zwei dieser Substitutionen offenbar von einander verschieden, und keine derselben kann der Reihe (1) angehören. Um diesen letzteren Punkt zu erweisen, genügt es, zu beachten, dass die Gleichung $S_i T_1 = S_j$ die folgende nach sich ziehen würde: $T_1 = S_i^{-1} S_j$, und diese ist deshalb unmöglich, weil das Produkt $S_i^{-1} S_j$ jedenfalls dem Systeme Γ angehört, während T_1 der Voraussetzung nach in (1) nicht vorkommt. Wir sehen somit, dass entweder $m = 2\mu$, oder $m > 2\mu$ ist. Wenn $m = 2\mu$ ist, so ist unser Satz erwiesen. Es sei daher $m > 2\mu$, und es bezeichne T_2 eine der Substitutionen von G, welche weder der Reihe (1), noch der Reihe (2) angehören. Werden die Substitutionen (1) zur Rechten mit T_2 multiplicirt, so erhält man die μ neuen Substitutionen

(3). $$T_2, S_1 T_2, S_2 T_2, \ldots, S_{\mu-1} T_2,$$

welche dem Systeme G angehören. Dieselben sind von einander und von den Substitutionen (1) verschieden. Ferner kann keine von ihnen gleich einer der Substitutionen (2) sein; wäre nämlich $S_i T_2 = S_j T_1$, so müsste $T_2 = S_i^{-1} S_j T_1$ sein, was der Voraussetzung widerspricht, da das Produkt $S_i^{-1} S_j T_1$ offenbar ein Glied der Reihe (2) ist. Man hat somit entweder $m = 3\mu$, oder $m > 3\mu$. Da man diese Schlüsse so lange fortsetzen kann, bis alle Substitutionen des Systems G erschöpft sind, so sieht man, dass

$$m = q\mu$$

sein muss, wo q eine ganze Zahl bezeichnet.

Anmerkung, — Das conjugirte System G ist auf diese Weise in q **Reihen** von Substitutionen

$$\begin{array}{lllll}
1 & , S_1 & , S_2 & , \ldots, & S_{\mu-1}, \\
T_1 & , S_1 T_1 & , S_2 T_1 & , \ldots, & S_{\mu-1} T_1 \quad , \\
T_2 & , S_1 T_2 & , S_2 T_2 & , \ldots, & S_{\mu-1} T_2 \quad , \\
\cdot & \cdot & \cdot & \cdot & \cdot \quad , \\
T_{q-1} & , S_1 T_{q-1} & , S_2 T_{q-1} & , \ldots, & S_{\mu-1} T_{q-1}
\end{array}$$

zerlegt worden, von denen die erste allein ein conjugirtes System ausmacht. Um diese Tabelle zu bilden, auf welcher unser Schlussverfahren beruht, haben wir die Substitutionen des Systems Γ der Reihe nach zur Rechten mit den Substitutionen $T_1, T_2, \ldots, T_{q-1}$ multiplicirt. Es ist aber zu beachten, dass wir noch auf eine andere Weise hätten verfahren können. Der Beweis lässt sich nämlich auch dadurch führen, dass man die Substitutionen des Systems Γ links mit Substitutionen $U_1, U_2, \ldots, U_{q-1}$ des Systems G multiplicirt. Bei diesem Verfahren wird das System G in q Reihen

$$\begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ U_1, & U_1 S_1, & U_1 S_2, & \ldots, & U_1 S_{\mu-1}, \\ U_2, & U_2 S_1, & U_2 S_2, & \ldots, & U_2 S_{\mu-1}, \\ \cdot & \cdot & \cdot & \cdot & \cdot \quad, \\ U_{q-1}, & U_{q-1} S_1, & U_{q-1} S_2, & \ldots, & U_{q-1} S_{\mu-1} \end{array}$$

zerlegt, deren jede wieder μ Substitutionen enthält. Jede Substitution U ist eine der Substitutionen von G, welche den bereits gebildeten Horizontalreihen nicht angehören.

414. Der vorhergehende Lehrsatz führt zu wichtigen Folgerungen, die in den folgenden Zusätzen enthalten sind:

Zusatz I. — Die Ordnung eines Systems conjugirter Substitutionen, die aus n Buchstaben gebildet sind, ist ein Divisor des Produkts $N = 1.2.3\ldots n$.

In der That gehören die Substitutionen des vorgelegten Systems dem conjugirten Systeme N^{ter} Ordnung an, welches alle Substitutionen der n Buchstaben umfasst.

Zusatz II. — Die Ordnung eines conjugirten Systems ist ein Vielfaches der Ordnung irgend einer der Substitutionen des Systems.

Die Potenzen einer der Substitutionen eines conjugirten Systems gehören sämmtlich diesem Systeme an. Diese Potenzen bilden ferner ein conjugirtes System, dessen Ordnung gleich derjenigen der Substitution ist. Folglich ist diese Ordnung ein Divisor der Ordnung des vorgelegten Systems.

Zusatz III. — Wenn die Anzahl n der Buchstaben eine Primzahl ist, so besteht jedes conjugirte System n^{ter} Ordnung aus den n Potenzen einer cyclischen Substitution n^{ter} Ordnung.

Die Ordnung irgend einer Substitution des Systems muss nämlich in n aufgehen; sie reducirt sich also auf 1, oder auf n.

Zusatz IV. — Wenn zwei conjugirte Systeme mehrere Substitutionen gemeinschaftlich haben, so bilden die letzteren ein conjugirtes System; ihre Anzahl ist folglich ein den Ordnungen der beiden gegebenen Systeme gemeinschaftlicher Divisor.

Es seien nämlich

$$(1). \qquad 1, S_1, S_2, \ldots, S_{\mu-1}$$

alle zwei conjugirten Systemen gemeinschaftlichen Substitutionen. Jede Substitution S, die durch irgendwelche Multiplicationen aus den Substitutionen (1) gebildet ist, gehört gleichzeitig den beiden vorgelegten Systemen an, und da letztere nur die μ Substitutionen (1) gemeinschaftlich haben, so muss die Substitution S sich in der Reihe (1) vorfinden; die Substitutionen (1) bilden daher ein conjugirtes System.

Aehnliche Systeme und gegeneinander vertauschbare Systeme.

415. Wir betrachten ein System conjugirter Substitutionen

$$(1). \qquad 1, S_1, S_2, \ldots, S_{\mu-1}.$$

Oben fanden wir das Resultat, dass TST^{-1} und S zwei ähnliche Substitutionen sind, die Substitution T mag sein, welche sie will, und dass es zur Bildung der Substitution TST^{-1} genügt, die Substitution T in den Cyclen von S auszuführen. Daraus geht hervor, dass die Substitutionen

$$(2). \qquad 1, TS_1T^{-1}, TS_2T^{-1}, \ldots, TS_{\mu-1}T^{-1}$$

ein conjugirtes System ausmachen. Man kann diese Thatsache auch unmittelbar bewahrheiten, wenn man beachtet, dass das Produkt irgend welcher Substitutionen der Reihe (2) die Form $TS_\alpha S_\beta \ldots S_\omega T^{-1}$, folglich, da die Substitutionen (1) der Voraussetzung nach ein conjugirtes System bilden, die Form TS_iT^{-1} hat.

Die conjugirten Systeme (1) und (2) sollen ähnliche Systeme genannt werden. Es kann der Fall eintreten, dass diese

beiden Systeme zusammenfallen; dann hat man für jeden Werth von i

$$TS_iT^{-1} = S_j \text{ oder } TS_i = S_jT.$$

Man erhält folglich dieselben Resultate, man mag die Substitutionen (1) zur Rechten oder zur Linken mit T multipliciren.

Wir betrachten jetzt zwei Systeme conjugirter Substitutionen:

$$1\ ,\ S_1\ ,\ S_2\ ,\ S_3\ ,\ \ldots\ ,\ S_{\mu-1}\ ,$$
$$1\ ,\ T_1\ ,\ T_2\ ,\ T_3\ ,\ \ldots\ ,\ T_{\nu-1}\ .$$

Wir werden sagen, diese Systeme seien gegeneinander vertauschbar, wenn jedes Produkt von der Form $T_j S_i$ zugleich von der Form $S_{i'}\ T_{j'}$ ist. Hat man für jeden Werth von i und von j $j' = j$, so fällt das erste der beiden vorgelegten Systeme mit dem ähnlichen Systeme zusammen, welches man daraus herleitet, wenn man seine Substitutionen zur Linken mit T_j, zur Rechten mit T_j^{-1} multiplicirt. Wenn für alle Werthe von i und j gleichzeitig $i' = i$, $j' = j$ ist, so sind irgend zwei aus beiden vorgelegten Systemen genommene Substitutionen gegeneinander vertauschbar.

Ueber das allgemeine Problem, welches den Hauptgegenstand der Theorie der Substitutionen bildet.

416. Das allgemeine Problem, welches in der Theorie der Substitutionen zu behandeln ist, lässt sich folgendermassen aussprechen:

Welches sind die Systeme conjugirter Substitutionen, die man aus n gegebenen Buchstaben bilden kann?

Die Lösung dieser schwierigen Aufgabe würde für die Algebra von der grössten Wichtigkeit sein; auch haben sich Lagrange und später mehrere hervorragende Mathematiker mit derselben beschäftigt. Trotz aller Bemühungen sind sie aber nicht zum Ziele gelangt, und die Wissenschaft besitzt bis jetzt über diesen Gegenstand nur eine geringe Anzahl allgemeiner Sätze, die wir im Folgenden herleiten wollen.

Von den Systemen conjugirter Substitutionen, die man aus n gegebenen Buchstaben bilden kann, kennen wir: 1^0 das System, welches die $N = 1.2\ldots n$ Substitutionen umfasst; 2^0 die

Systeme, welche man dadurch erhält, dass man alle Potenzen irgend einer Substitution nimmt. Wir machen hierauf nochmals aufmerksam, um alle erhaltenen Resultate hier vorzuführen.

417. Lehrsatz I. — Diejenigen der $N = 1.2.3\ldots n$ aus n gegebenen Buchstaben möglichen Substitutionen, welche einer geraden Anzahl von Transpositionen äquivalent sind, machen ein conjugirtes System der Ordnung $\frac{N}{2}$ aus, und es giebt kein anderes conjugirtes System von derselben Ordnung $\frac{N}{2}$.

Der erste Theil des Satzes leuchtet unmittelbar ein. Wir haben nämlich gesehen, dass man durch Multiplication mehrerer Substitutionen erster Art, d. h. mehrerer Substitutionen, von denen jede einer geraden Anzahl von Transpositionen äquivalent ist, eine Substitution erster Art erhält.

Um den zweiten Theil des Satzes zu beweisen, nehmen wir an, es sei

$$(1). \qquad 1\ ,\ S_1\ ,\ S_2\ ,\ S_3\ ,\ \ldots\ ,\ S_{\frac{N}{2}-1}$$

ein conjugirtes System der Ordnung $\frac{N}{2}$. Multipliciren wir die Substitutionen dieses Systems zur Linken und zur Rechten mit einer beliebigen Substitution T, so erhalten wir die Produkte

$$(2). \qquad T\ ,\ TS_1\ ,\ TS_2\ ,\ TS_3\ ,\ \ldots\ ,\ TS_{\frac{N}{2}-1}$$

und

$$(3). \qquad T\ ,\ S_1T\ ,\ S_2T\ ,\ S_3T\ ,\ \ldots\ ,\ S_{\frac{N}{2}-1}T.$$

Wenn T dem Systeme (1) angehört, so bilden die Reihen (2) und (3) conjugirte Systeme, welche mit (1) identisch sind. Wenn aber T nicht in (1) enthalten ist, so besteht, wie wir oben gesehen haben, jede der Reihen (2) und (3) aus den $\frac{N}{2}$ Substitutionen, welche dem System (1) nicht angehören. In allen Fällen enthalten die Reihen (2) und (3) dieselben Substitutionen, und man hat folglich für jeden Werth von i und für einen gewissen Werth von j

$$TS_i = S_jT \text{ oder } TS_iT^{-1} = S_j.$$

Daraus geht hervor, dass das System (1) alle Substitutionen umfasst, welche irgend einer der darin enthaltenen ähnlich sind.

Es kann daher keine der Transpositionen diesem Systeme angehören; denn sonst müsste es dieselben sämmtlich enthalten, und seine Ordnung würde im Widerspruch mit unserer Voraussetzung gleich N sein.

Wenn jetzt T eine Transposition bezeichnet, so enthalten die Reihen (1) und (2) alle N Substitutionen der n Buchstaben, und diese Substitutionen vertauschen sich nur gegeneinander, wenn man sie mit einer Transposition U multiplicirt. Nun ist nach dem Vorhergehenden klar, dass sich die Reihe (1) in Folge dieser Multiplication in (2) verwandelt; folglich verwandelt sich die Reihe (2) in (1), woraus hervorgeht, dass die Substitution UT dem Systeme (1) angehört. Dieses System umfasst danach alle Substitutionen, welche Produkte von je zwei Transpositionen sind; es enthält mithin die $\frac{N}{2}$ Substitutionen, von denen jede irgend einer geraden Anzahl von Transpositionen äquivalent ist.

Zusatz.— Das conjugirte System der Ordnung $\frac{N}{2}$ enthält alle cyclischen Substitutionen ungerader, und keine einzige cyclische Substitution gerader Ordnung.

Jede cyclische Substitution p^{ter} Ordnung ist nämlich $p-1$ Transpositionen äquivalent; man hat

$$(a_0, a_1, a_2, \ldots, a_{p-1}) = (a_0, a_{p-1})(a_0, a_{p-2}) \ldots (a_0, a_2)(a_0, a_1).$$

418. Lehrsatz II. — Wenn ein conjugirtes System alle cyclischen Substitutionen umfasst, deren Ordnung eine gegebene Zahl $p = n$ oder $< n$ ist, so ist seine Ordnung N oder $\frac{N}{2}$. Die Ordnung des Systems ist immer gleich N, wenn p eine gerade Zahl ist.

Die Wahrheit des Satzes liegt auf der Hand, wenn $p = 2$ ist; denn das vorgelegte System enthält dann alle Transpositionen, und seine Ordnung ist gleich N. Wenn $p = 3$ ist, so enthält das vorgelegte System die cyclische Substitution

$$(a_1, a_2, a_3) = (a_1, a_3)(a_1, a_2)$$

der drei gegebenen Buchstaben a_1, a_2, a_3; dasselbe enthält auch, wenn die Zahl $n > 3$ ist, und a_4 einen neuen Buchstaben bezeichnet, die Substitution

$$(a_4, a_3, a_1) = (a_3, a_4)(a_1, a_3).$$

Wird die erste Substitution mit der zweiten multiplicirt, so erhält man

$$(a_3 \,,\, a_4)\ (a_1 \,,\, a_2)\,,$$

und dies Produkt muss in dem vorgelegten Systeme vorkommen. Das System enthält daher alle Substitutionen, welche einer geraden Anzahl von Transpositionen äquivalent sind, und seine Ordnung ist mithin wenigstens gleich $\frac{N}{2}$; ausserdem ist diese Ordnung ein Divisor von N; folglich ist sie gleich $\frac{N}{2}$, oder gleich N.

Der Fall, in welchem $p > 3$ ist, lässt sich auf den Fall $p = 3$ leicht zurückführen. Es seien a_1, a_2, a_3 drei beliebige der gegebenen Buchstaben, und es werde

$$T = (a_1 \,,\, a_2 \,,\, a_3) = (a_1 \,,\, a_3)\ (a_1 \,,\, a_2)$$

gesetzt; ferner sei

$$S = (a_1 \,,\, a_2 \,,\, b_4 \,,\, b_5 \,,\, \ldots \,,\, b_p \,,\, a_3)$$

eine cyclische Substitution p^{ter} Ordnung, welche aus den Buchstaben a_1, a_2, a_3 und aus $p - 3$ anderen gegebenen Buchstaben b_4, b_5, ..., b_p gebildet ist. Man erhält

$$(a_1 \,,\, a_2)\ S = (a_1)\ (a_2 \,,\, b_4 \,,\, b_5 \,,\, \ldots \,,\, b_p \,,\, a_3)\,,$$

und, wenn zur Linken mit $(a_1 \,,\, a_3)$ multiplicirt wird,

$$TS = (a_1 \,,\, a_3 \,,\, a_2 \,,\, b_4 \,,\, b_5 \,,\, \ldots \,,\, b_p).$$

Der Voraussetzung nach umfasst das vorgelegte System alle cyclischen Substitutionen p^{ter} Ordnung; folglich müssen darin die Substitutionen TS und S^{-1} vorkommen, und ebenso beider Produkt T, welches irgend eine der aus dreien der gegebenen Buchstaben gebildeten cyclischen Substitutionen ist.

Wenn die Zahl p gerade ist, so enthält das vorgelegte System die Produkte von Transpositionen, welche den cyclischen Substitutionen p^{ter} Ordnung äquivalent sind, in ungerader Anzahl; die Ordnung dieses Systems ist daher grösser als $\frac{N}{2}$, also gleich N.

419. Lehrsatz III. — *Wenn aus n Buchstaben irgend eine Substitution T gebildet ist, so machen die verschiedenen Substitutionen derselben Buchstaben, die gegen T vertauschbar sind, ein conjugirtes System aus.*

Es seien

$$1\ ,\ S_1\ ,\ S_2\ ,\ \ldots\ ,\ S_{M-1}$$

die M gegen T vertauschbaren Substitutionen, unter denen offenbar die Einheit enthalten sein muss. Wir haben gesehen, dass das Produkt mehrerer dieser Substitutionen selbst eine gegen T vertauschbare Substitution ist. Dies Produkt ist daher ein Glied der vorstehenden Reihe, und diese bildet somit ein conjugirtes System M^{ter} Ordnung. Die Zahl M hat (No. 402) den Werth

$$M = (1.2\ldots m_1)(1.2\ldots m_2)\ldots(1.2\ldots m_\omega)\, n_1^{m_1} n_2^{m_2} \ldots n_\omega^{m_\omega},$$

wo m_i die Anzahl der Cyclen von T bezeichnet, deren Ordnung gleich n_i ist. Hierbei werden die aus einem einzigen Buchstaben bestehenden Cyclen mitgezählt, so dass die Relation besteht:

$$n = m_1 n_1 + m_2 n_2 + \cdots + m_\omega n_\omega.$$

Ist im Besonderen die Anzahl n der Buchstaben gleich $m_1 n_1$, so kann man daraus nach dem vorstehenden Satze ein conjugirtes System der Ordnung

$$1.2.3\ldots m_1 \times n_1^{m_1}$$

bilden.

Beispiel. — Wenn

$$n = 6 = 3 \times 2 = 2 \times 3$$

ist, so lassen sich zwei Systeme conjugirter Substitutionen bilden, deren Ordnungen beziehungsweise $1.2.3 \times 2^3 = 48$ und $1.2 \times 3^2 = 18$ sind.

420. Lehrsatz IV. — Wenn aus n Buchstaben irgend eine Substitution T gebildet ist, so machen die verschiedenen Substitutionen S, für welche das Produkt STS^{-1} sich auf eine Potenz von T reducirt, ein System conjugirter Substitutionen aus.

Es stelle i eine gegebene Zahl dar, welche prim zur Ordnung der Substitution T ist. Die Anzahl der Substitutionen, die der Gleichung

$$STS^{-1} = T^i$$

genügen, ist (No. 409) gleich der Anzahl M der gegen S vertauschbaren Substitutionen. Bezeichnet man daher mit ν die Anzahl der Substitutionen S, welche die vorhergehende Gleichung befriedigen, wenn i aufhört, eine gegebene Zahl zu sein, und

mit $\varphi(\mu)$ die Zahl, welche anzeigt, wie viele Zahlen prim zur Ordnung μ der Substitution T und nicht grösser als μ sind, so hat man

$$\nu = M\,\varphi(\mu).$$

Dies vorausgesetzt, seien

$$(1). \qquad 1\,,\, S_1\,,\, S_2\,,\, S_3\,,\, \ldots\,,\, S_{\nu-1}$$

die Substitutionen, welche der im Ausspruch des Satzes angegebenen Bedingung genügen. Wir behaupten, dass das Produkt von zwei beliebigen der Substitutionen (1) sich in derselben Reihe vorfindet, dass diese Reihe folglich ein conjugirtes System ν^{ter} Ordnung bildet. Dies zu beweisen, betrachten wir die beiden Substitutionen S_1, S_2. Der Voraussetzung nach ist

$$(2). \qquad S_1\,T\,S_1^{-1} = T^i, \text{ oder } S_1\,T = T^i\,S_1\,,$$

$$(3). \qquad S_2\,T\,S_2^{-1} = T^j, \text{ oder } S_2\,T = T^j S_2.$$

Wird die Gleichung (3) zur Linken mit S_1 multiplicirt, so folgt

$$(4). \qquad S_1\,S_2\,T = S_1\,T^j\,S_2\,,$$

und wenn man die Gleichung (2) auf die Potenz j erhebt, so erhält man

$$S_1\,T\,S_1^{-1}\,.\,S_1\,T\,S_1^{-1}\,\ldots\,S_1\,T\,S_1^{-1} = T^{ij}\,,$$

das heisst

$$(5). \qquad S_1\,T^j\,S_1^{-1} = T^{ij}, \text{ oder } S_1\,T^j = T^{ij}\,S_1.$$

Mit Rücksicht auf diese Gleichung (5) liefert die Formel (4):

$$(6). \qquad S_1\,S_2\,T = T^{ij}\,S_1\,S_2 \text{ oder } (S_1\,S_2)\,T\,(S_1\,S_2)^{-1} = T^{ij}\,,$$

woraus die Richtigkeit unserer Behauptung, $S_1\,S_2$ sei in der Reihe (1) enthalten, hervorgeht.

421. Es seien e eine der Zahlen, die prim zu μ sind, und ϑ der Exponent, zu welchem e nach dem Modul μ gehört. Wenn man die Reihe (1) nicht mehr aus allen Substitutionen S bestehen lässt, welche der Gleichung

$$S\,T\,S^{-1} = T^i$$

für einen beliebigen Werth von i genügen, sondern nur diejenigen Substitutionen S nimmt, welche dieselbe Gleichung unter der Voraussetzung befriedigen, dass i nach dem Modul μ einer Potenz von e congruent sei, so bilden diese Substitutionen (1) gleichfalls ein conjugirtes System. Setzt man nämlich voraus, dass i

und j in den Gleichungen (2) und (3) zwei Potenzen von e bezeichnen, so ist auch das Produkt ij eine Potenz von e, und der Formel (6) wegen gehört das Produkt $S_1 S_2$ der Reihe (1) an. Wir gelangen somit zu dem folgenden Satze:

Lehrsatz V. — Hat man aus n Buchstaben irgend eine Substitution μ^{ter} Ordnung T gebildet, und bildet sodann alle Substitutionen S von der Beschaffenheit, dass das Produkt STS^{-1} sich auf eine Potenz von T reducire, deren Exponent nach dem Modul μ congruent ist einer Potenz einer nach dem Modul μ zum Exponenten ϑ gehörenden gegebenen Zahl e, so machen die Substitutionen S ein conjugirtes System der Ordnung ϑM aus. Wenn die Zahl μ primitive Wurzeln hat, so kann ϑ irgend ein Divisor von $\varphi(\mu)$ sein.

Dieser Lehrsatz V umfasst den Lehrsatz III als einen besonderen Fall; beide fallen zusammen, wenn man $\vartheta = 1$, folglich $e = 1$ macht. Der Satz V enthält aber nicht den Satz IV, da eine zusammengesetzte Zahl im Allgemeinen keine primitive Wurzel besitzt. Diese Ausdehnung des Lehrsatzes III ist von Jordan im XXXVIII^ten^ Hefte des Journal de l'École Polytechnique angegeben worden.

Zusatz I. — Man kann aus n Buchstaben Systeme conjugirter Substitutionen der Ordnung $n\varphi(n)$ und der Ordnung $\frac{n\varphi(n)}{t}$ bilden, wo t ein passend gewählter Divisor von n ist. Wenn im Besonderen n eine Primzahl ist, so kann man ein System conjugirter Substitutionen bilden, dessen Ordnung gleich $n(n-1)$ oder gleich dem Quotienten dieser Zahl durch irgend einen Divisor von $n-1$ ist.

Dieser Zusatz geht unmittelbar aus den Sätzen IV und V hervor, wenn man darin T eine cyclische Substitution n^{ter} Ordnung bedeuten lässt.

Zusatz II. — Man kann aus $n-1$ gegebenen Buchstaben ein conjugirtes System der Ordnung $\varphi(n)$ oder $\frac{\varphi(n)}{t}$ bilden.

Wir betrachten das conjugirte System, welches $n\varphi(n)$ oder $\frac{n\varphi(n)}{t}$ Substitutionen von n Buchstaben enthält, und von dem im

vorhergehenden Zusatze die Rede ist. Um dieses System zu bilden, geht man von einer cyclischen Substitution n^{ter} Ordnung T aus und nimmt die Substitutionen S, welche einer Gleichung von der Form $STS^{-1} = T^i$ genügen. Nun geht aus der Bildungsweise dieser Substitutionen S hervor, dass es für jeden Werth von i eine einzige Substitution S giebt, welche einen gegebenen Buchstaben a nicht versetzt. Folglich enthält das betrachtete System $\varphi(n)$ oder $\frac{\varphi(n)}{t}$ Substitutionen, welche nur $n-1$ Buchstaben versetzen, und es liegt auf der Hand, dass diese Substitutionen ein conjugirtes System ausmachen.

422. Lässt man, falls $n = 6$ ist, T zunächst eine regelmässige Substitution bedeuten, welche aus zwei Cyclen dritter Ordnung besteht, so kann man nach dem Lehrsatz IV ein System conjugirter Substitutionen bilden, dessen Ordnung $1.2 \times 3^2 \times 2$ oder 36 ist. Nimmt man zweitens für T eine cyclische Substitution 6ter Ordnung, so kann man nach dem Lehrsatz V (Zusatz I) ein conjugirtes System der Ordnung $6 \times \varphi(6)$ oder 12 bilden. Es sei

$$T = (a, b, c, d, e, f)$$

die gewählte cyclische Substitution; dann besteht das conjugirte System

1° aus den sechs Potenzen von T

$$1, T, T^2, T^3, T^4, T^5;$$

2° aus den folgenden sechs Substitutionen zweiter Ordnung:

$$(a, b)(c, f)(d, e) \quad , \quad (a, c)(d, f)(b)(e),$$
$$(a, d)(b, c)(e, f) \quad , \quad (a, e)(b, d)(c)(f),$$
$$(a, f)(b, e)(c, d) \quad , \quad (b, f)(c, e)(a)(d).$$

Bezeichnet S irgend eine dieser sechs letzten Substitutionen, so ist

$$STS^{-1} = T^5 \text{ oder } (ST)^2 = 1.$$

423. Lehrsatz VI. — Wenn zwei Systeme conjugirter Substitutionen

$$1, S_1, S_2, \ldots, S_{\mu-1},$$
$$1, T_1, T_2, \ldots, T_{\nu-1},$$

deren Ordnungen beziehungsweise μ und ν sind, gegeneinander vertauschbar sind und keine Substitution gemeinschaftlich haben, so bilden die Substitutionen

$$\begin{array}{lllll} 1 & , S_1 & , S_2 & , \ldots , & S_{\mu-1} \quad , \\ T_1 & , T_1 S_1 & , T_1 S_2 & , \ldots , & T_1 S_{\mu-1} , \\ T_2 & , T_2 S_1 & , T_2 S_2 & , \ldots , & T_2 S_{\mu-1} , \\ . & . & . & . & . \quad , \\ T_{\nu-1} , & T_{\nu-1} S_1 & , T_{\nu-1} S_2 & , \ldots , & T_{\nu-1} S_{\mu-1} , \end{array}$$

oder

$$\begin{array}{lllll} 1 & , S_1 & , S_2 & , \ldots , & S_{\mu-1} \quad , \\ T_1 & , S_1 T_1 & , S_2 T_1 & , \ldots , & S_{\mu-1} T_1 \quad , \\ T_2 & , S_1 T_2 & , S_2 T_2 & , \ldots , & S_{\mu-1} T_2 \\ . & . & . & . & . \quad , \\ T_{\nu-1} & , S_1 T_{\nu-1} & , S_2 T_{\nu-1} & , \ldots , & S_{\mu-1} T_{\nu-1} , \end{array}$$

welche durch Multiplication der Substitutionen des einen Systems mit denjenigen des zweiten Systems entstehen, ein conjugirtes System der Ordnung $\mu\nu$.

Multiplicirt man nämlich mehrere Terme irgend einer der beiden Tabellen, so erhält man ein aus Factoren T und aus Factoren S zusammengesetztes Produkt. Man kann aber der Voraussetzung nach die Reihenfolge zweier aufeinander folgenden Factoren S und T umkehren, vorausgesetzt, dass man zugleich die Indices ändert; denn es ist für jeden Werth von i und von j

$$S_i T_j = T_{j'} S_{i'} \text{ und } T_j S_i = S_{i'} T_{j'} .$$

Ausserdem reducirt sich das Produkt mehrerer aufeinanderfolgenden Factoren S oder T auf eine der mit S oder T bezeichneten Substitutionen. Das Produkt, welches wir gebildet haben, ist mithin von einer der beiden Formen

$$S_i T_j \quad , \quad T_j S_i ,$$

und es kommt folglich in jeder unserer Tabellen vor. Wir haben jetzt noch zu zeigen, dass zwei Substitutionen ein und derselben Tabelle verschieden sind: Die Gleichung

$$T_i S_j = T_{i'} S_{j'}$$

zieht die folgende nach sich:

$$S_j S_{j'}^{-1} = T_{i'} T_i^{-1} .$$

Das erste Glied dieser Relation gehört dem Systeme S, das zweite dem Systeme T an; ferner haben diese beiden Systeme nur den Term 1 gemeinschaftlich. Man hat daher

$$S_j\, S_j'^{-1} = 1 \ , \ T_i'\, T_i^{-1} = 1,$$

das heisst

$$S_j' = S_j \ , \ T_i' = T_i .$$

Jede unserer Tabellen umfasst mithin $\mu\nu$ verschiedene Substitutionen, welche ein conjugirtes System ausmachen.

Zusatz I. — Wenn die Substitutionen S und T, deren Ordnungen beziehungsweise μ und ν seien, gegeneinander vertauschbar sind und keine Potenz ausser der Einheit gemeinschaftlich haben, so erhält man ein conjugirtes System der Ordnung $\mu\nu$, wenn man die μ Potenzen von S mit den ν Potenzen von T multiplicirt.

Unter der gemachten Voraussetzung erfüllen nämlich die beiden conjugirten Systeme

$$1 \ , \ S \ , \ S^2 \ , \ \ldots \ , \ S^{\mu-1} ,$$

$$1 \ , \ T \ , \ T^2 \ , \ \ldots \ , \ T^{\nu-1}$$

die im vorstehenden Lehrsatze angegebenen Bedingungen.

Zusatz II. — Wenn mehrere Substitutionen $S, T, U, \ldots$, deren Ordnungen beziehungsweise $\mu, \nu, \varrho, \ldots$ seien, zu je zweien gegeneinander vertauschbar sind, und wenn die Gleichung

$$S^i\, T^j\, U^k \ldots = 1$$

nur für die Werthe $i = \mu$, $j = \nu$, $k = \varrho$, ... stattfinden kann, so erhält man ein conjugirtes System der Ordnung $\mu\nu\varrho \ldots$, wenn man die Potenzen von S mit denjenigen von T, die so erhaltenen Resultate mit den Potenzen von U, u. s. w. multiplicirt.

Anmerkung. — Wenn

$$P = (a_0 , a_1 , \ldots , a_{\varrho-1})\ (b_0 , b_1 , \ldots , b_{\varrho-1})\ \ldots\ (f_0 , f_1 , \ldots , f_{\varrho-1}),$$

$$Q = (a_0 , b_0 , \ldots , f_0)\ (a_1 , b_1 , \ldots , f_1)\ \ldots\ (a_{\varrho-1} , b_{\varrho-1} , \ldots , f_{\varrho-1})$$

gesetzt wird, und wenn S und T zwei gegeneinander vertauschbare Substitutionen sein sollen, welche keine Potenz ausser der Einheit gemeinschaftlich haben, so ist erforderlich und hinreichend, dass (No. 405)

$$S = P \ , \ T = Q ,$$

oder

$$S = PP'P'' \ldots, \quad T = QQ'Q'' \ldots$$

sei, worin P' und Q', P'' und Q'', ... Substitutionen bezeichnen, welche auf dieselbe Weise wie P und Q, aber aus verschiedenen Buchstaben gebildet sind.

Betrachten wir z. B. den Fall, in welchem 6 Buchstaben gegeben sind. Macht man

$$S = (a, b)\,(c, d)\,(e, f) \quad , \quad T = (a, c)\,(b, d)\,(e)\,(f),$$

so erhält man ein conjugirtes System vierter Ordnung, welches aus folgenden vier Substitutionen besteht:

$$1, S, T, ST.$$

424. Untersuchung eines bemerkenswerthen Falles, welcher in die Lehrsätze V und VI eingeht. — Der Fall, um den es sich hier handelt, ist derjenige des Systems von $n\,(n-1)$ conjugirten Substitutionen, von welchem im Zusatz I zum Lehrsatz V die Rede ist, wenn n eine Primzahl bedeutet.

Es seien

$$a_0, a_1, a_2, \ldots, a_{n-1}$$

die n gegebenen Buchstaben, und es werde, wie in No. 404, vorausgesetzt, dass a_{nq+r} denselben Buchstaben wie a_r bezeichne. Das System, welches wir betrachten, besteht aus allen Substitutionen S, welche einer Gleichung von der Form

$$STS^{-1} = T^i$$

genügen, wo T eine cyclische Substitution n^{ter} Ordnung bezeichnet. Diese Substitution sei

$$T = (a_0, a_1, a_2, \ldots, a_{n-1}).$$

Da n eine Primzahl ist, und i irgend eine durch n nicht theilbare Zahl bezeichnet, so ist T^i eine cyclische Substitution n^{ter} Ordnung, und man hat den getroffenen Bestimmungen zufolge

$$T^i = [a_0, a_i, a_{2i}, \ldots, a_{(n-1)i}],$$

oder, wenn man einen beliebigen Buchstaben a_{ki} auf den ersten Platz bringt,

$$T^i = [a_{ki}, a_{(k+1)i}, \ldots, a_{(n-1)i}, a_0, a_i, \ldots, a_{(k-1)i}].$$

Dies vorausgesetzt, muss jede Substitution S dadurch gebildet werden, dass man zum Zähler die Permutation nimmt, welche den Cyclus von T^i, und zum Nenner die Permutation, welche den Cyclus von T ausmacht. Wir bezeichnen diese letzte Per-

mutation mit C und mit C', C'' die Permutationen, welche den Cyclus von T^i bilden, wenn man beziehungsweise a_0, a_{ki} auf den ersten Platz setzt. Der allgemeine Ausdruck der Substitutionen S ist dann

$$S = \binom{C''}{C} = \binom{C''}{C'}\binom{C'}{C}\cdot$$

Offenbar hat man

$$\binom{C''}{C'} = [a_0, a_{ki}, a_{2ki}, \ldots, a_{(n-1)ki}] = T^{ki}.$$

Was die Substitution $\binom{C'}{C}$ betrifft, so schliesst dieselbe den Buchstaben a_0 nicht ein, und es ist

$$\binom{C'}{C} = \begin{bmatrix} a_i\, a_{2i} \ldots a_{(n-1)i} \\ a_1\, a_2 \ldots a_{n-1} \end{bmatrix}.$$

Die Wirkung dieser Substitution besteht darin, dass die Indices der Buchstaben a mit i multiplicirt werden. Wir lassen jetzt r eine primitive Wurzel der Primzahl n bedeuten, setzen

$$i \equiv r^\nu \ (mod.\ n)$$

und bezeichnen mit U die Substitution, in Folge welcher die Indices der Buchstaben a mit r multiplicirt werden: dann ist klar, dass die ν^{te} Potenz von U diese Indices mit r^ν oder i multiplicirt; man hat daher

$$\binom{C'}{C} = U^\nu.$$

Ausserdem lehrt die Relation $r^{n-1} \equiv 1, (mod.\ n)$, dass U eine cyclische Substitution der Ordnung $n-1$ ist, deren Ausdruck folgender ist:

$$U = (a_1, a_r, a_{r^2}, a_{r^3}, \ldots, a_{r^{n-2}}).$$

Bezeichnet also h eine Zahl von der Beschaffenheit, dass $h \equiv ki$ $(mod.\ n)$ ist, so hat die Substitution S den Werth:

$$S = T^h U^\nu. \qquad (1).$$

Aus der Gleichung

$$STS^{-1} = T^i$$

ergiebt sich endlich

$$ST^kS^{-1} = T^{ki} = T^h = SU^{-\nu},$$

also

$$T^k S^{-1} = U^{-\nu}$$

und

(2). $$S = U^{\nu} T^{k}.$$

Die Formeln (1) und (2) liefern mithin denselben Werth von S, wenn die Exponenten h und k der Relation

$$h = k r^{\nu}$$

genügen. Jede derselben giebt uns alle Substitutionen des in Rede stehenden Systems, wenn man darin h oder k die n Werthe $0, 1, 2, \ldots, n-1$ und ν dieselben Werthe mit Ausnahme von Null, oder, was auf dasselbe hinausläuft, mit Ausnahme von $n-1$ ertheilt. Mit andern Worten: man erhält das System, mit dem wir uns beschäftigen, dadurch, dass man die Substitutionen

$$1, T, T^2, \ldots, T^{n-1}$$

zur Rechten oder zur Linken mit den Substitutionen

$$1, U, U^2, \ldots, U^{n-2}$$

multiplicirt.

Beispiel. — Wir betrachten den Fall, in welchem $n = 5$ ist. Da 5 die primitive Wurzel 2 besitzt, so kann man durch Multiplication der Potenzen der beiden Substitutionen

$$T = (a_0, a_1, a_2, a_3, a_4), \quad U = (a_1, a_2, a_4, a_3)$$

ein System von zwanzig conjugirten Substitutionen bilden. Es ist leicht, an diesem Beispiel zu zeigen, dass die Formel

$$U^{\nu} T^{k} U^{-\nu} = T^{k.2^{\nu}}$$

für alle Werthe der Zahlen k und ν stattfindet.

425. Lehrsatz VII. — Es ist ein System von n Buchstaben gegeben, und es seien n_1 eine ganze Zahl, die gleich n oder kleiner als n ist, $\nu = m_1 n_1$ ein in n enthaltenes Vielfache von n_1. Ferner sei n_2 eine Zahl, die gleich m_1 oder kleiner als m_1 ist, und $m_2 n_2$ ein in m_1 enthaltenes Vielfache von n_2. Ebenso sei n_3 eine Zahl, die gleich m_2 oder kleiner als m_2 ist, und $m_3 n_3$ ein in m_2 enthaltenes Vielfache von n_3, u. s. w. Dann kann man aus ν Buchstaben, die nach Belieben aus der Reihe der gegebenen n Buchstaben gewählt sind, stets ein System conjugirter Substitutionen bilden, dessen Ordnung $n_1^{m_1} n_2^{m_2} n_3^{m_3} \ldots$ ist.

Dieser Satz ist von Cauchy in der bereits citirten Arbeit bewiesen.

Wir nehmen $\nu = m_1 n_1$ Buchstaben aus der Reihe der gegebenen, und vertheilen dieselben in m_1 Gruppen, deren jede aus n_1 Buchstaben besteht, und die wir Gruppen erster Art nennen wollen. Darauf setzen wir aus diesen m_1 Gruppen die Cyclen von m_1 cyclischen Substitutionen der Ordnung n_1 zusammen, die wir durch

(1). $$P_1 , P_2 , P_3 , \ldots , P_{m_1}$$

darstellen.

Von den m_1 Gruppen erster Art nehmen wir $m_2 n_2$ und vertheilen dieselben in m_2 Gruppen zweiter Art, welche danach durch die Vereinigung von n_2 Gruppen erster Art gebildet werden. Aus den $n_1 n_2$ Buchstaben jeder Gruppe zweiter Art bilden wir eine Substitution, welche die Wirkung hat, die in der Gruppe zweiter Art enthaltenen Gruppen erster Art cyclisch zu versetzen; die so erhaltenen m_2 Substitionen seien

(2). $$Q_1 , Q_2 , Q_3 , \ldots , Q_{m_2}.$$

Wenn $C , C' , C'', \ldots$ die Gruppen erster Art bezeichnen, welche eine Gruppe zweiter Art zusammensetzen, so ist jede Substitution (2) von der Form

$$(C\,C'\,C''\ldots) \quad \text{oder} \quad \begin{pmatrix} C' & C'' & C''' & \ldots \\ C & C' & C'' & \ldots \end{pmatrix}.$$

Ihre Wirkung besteht darin, dass jeder Buchstabe von C durch denjenigen ersetzt wird, welcher in C' denselben Platz einnimmt, dass an die Stelle des letzteren derjenige tritt, welcher denselben Platz in C'' einnimmt, u. s. w. Daraus geht hervor, dass die Substitutionen Q regelmässig sind, und dass jede von ihnen aus n_1 Cyclen der Ordnung n_2 besteht.

Von den m_2 Gruppen zweiter Art nehmen wir $m_3 n_3$ und vertheilen sie in m_3 Gruppen dritter Art, welche danach n_3 Gruppen zweiter Art enthalten. Aus den $n_1 n_2 n_3$ Buchstaben jeder Gruppe dritter Art bilden wir eine Substitution, welche die Wirkung hat, die in der Gruppe dritter Art enthaltenen Gruppen zweiter Art cyclisch zu versetzen. Die so erhaltenen m_3 Substitutionen seien

(3). $$R_1 , R_2 , R_3 , \ldots , R_{m_3}.$$

Durch Wiederholung des hinsichtlich der Substitutionen Q ange-

stellten Schlussverfahrens beweist man, dass jede Substitution R regelmässig ist und aus $n_1 n_2$ Cyclen der Ordnung n_3 besteht. Auf diese Weise kann man so lange fortfahren, bis in der Reihe der Zahlen m_1, m_2, m_3, ... die Einheit zum Vorschein kommt.

In jeder der Reihen (1), (2), (3), ... haben irgend zwei Substitutionen keinen Buchstaben gemeinschaftlich; sie sind folglich gegeneinander vertauschbar. Man erhält also ein System conjugirter Substitutionen P der Ordnung $n_1^{m_1}$, indem man die m_1 Reihen, deren jede aus den n_1 Potenzen einer der Substitutionen (1) gebildet ist, in einander multiplicirt. Auf dieselbe Weise entstehen aus den Substitutionen (2), (3), ... conjugirte Systeme Q, R, ..., deren Ordnungen beziehungsweise $n_2^{m_2}, n_3^{m_3}, \ldots$ sind.

Wir behaupten ferner, irgend zwei der so gebildeten Systeme seien gegeneinander vertauschbar. Dies zu beweisen, stellen wir die Buchstaben, welche in jeder der verschiedenen Gruppen irgend einer Art enthalten sind, durch ein und dasselbe Zeichen a, oder b, oder c, ... dar, dem wir einen veränderlichen Index anhängen. Dann können diejenigen der Substitutionen P, Q, R, ..., welche die Wirkung haben, die in einer der betrachteten Gruppen enthaltenen Gruppen niedrigerer Arten cyclisch zu vertauschen, aus den auf eine andere Gruppe bezüglichen dadurch hergeleitet werden, dass man das mit Indices versehene Zeichen ändert, die Indices aber unverändert lässt. Wenn demnach A und B zwei Gruppen i^{ter} Art bezeichnen, welche beziehungsweise aus den mit denselben Indices versehenen Buchstaben a, b gebildet sind, und wenn eine der Substitutionen P, Q, ... A in A' verwandelt, so verwandelt eine dieser Substitutionen auch B in B', und die Reihenfolge der Indices von b in B' ist dieselbe, wie die Reihenfolge der Indices von a in A'.

Dies vorausgesetzt, sei V eine Substitution einer der Reihen (2), (3), ..., welche die in einer Gruppe $(i+1)^{\text{ter}}$ Art $ABCD \ldots K$ enthaltenen Gruppen i^{ter} Art $A, B, C, D, \ldots, K$ cyclisch versetzt. Zugleich sei U eine der Substitutionen (1), (2), (3), ..., welche nur in einer der Gruppen A, B, ..., z. B. in C Buchstabenversetzungen hervorbringen. Wir nehmen an, U verwandle C in C'; nach dem eben Gesagten enthält das System, welchem U angehört, eine andere Substitution U', welche auch D in D' ver-

wandelt. Wir wollen nun der Reihe nach jede der drei Substitutionen U, V, U'^{-1} auf die Gruppirung

$$A\,B\,C\,D\ldots K$$

anwenden. In Folge der Substitution U geht dieselbe zunächst über in

$$A\,B\,C'\,D\ldots K;$$

wendet man sodann die Substitution V an, so ergiebt sich

$$B\,C\,D'\ldots K\,A;$$

endlich erhält man mittels der Substitution U'^{-1}, da diese D' in D verwandelt,

$$B\,C\,D\ldots A.$$

Zu genau demselben Resultat würde man gelangt sein, wenn man die Substitution V auf die anfängliche Gruppirung angewandt hätte; es ist daher

$$U'^{-1}\,V\,U = V\text{, folglich } V\,U = U'\,V.$$

Daraus geht hervor, dass die conjugirten Systeme $P, Q, R, \ldots$ zu je zweien gegeneinander vertauschbar sind. Ausserdem kann ein Produkt von der Form $V\ldots R\,Q\,P$, welches aus Substitutionen dieser verschiedenen Systeme gebildet ist, sich nicht auf die Einheit reduciren, wofern nicht jeder seiner Factoren gleich Eins wird; denn sonst hätte man

$$\ldots R\,P\,Q = V^{-1},$$

was deshalb unmöglich ist, weil die im ersten Gliede enthaltene Substitution die Buchstaben-Gruppen, welche V^{-1} gegeneinander vertauscht, nicht versetzen kann. Man erhält somit durch Multiplication der Systeme $P, Q, R, \ldots$ ein System conjugirter Substitutionen der Ordnung $n_1^{m_1}\,n_2^{m_2}\,n_3^{m_3}\ldots$.

Zusatz I. — Es ist ein System von n Buchstaben gegeben, und es bezeichne p eine Primzahl, die gleich n oder kleiner als n ist. Ferner seien $\nu = m_1 p$ ein in n enthaltenes Vielfache von p, $m_2 p$ ein in m_1 enthaltenes Vielfache von p, $m_3 p$ ein in m_2 enthaltenes Vielfache von p, u. s. w. Dann kann man aus ν nach Belieben gewählten Buchstaben immer ein System primitiver und conjugirter Substitutionen bilden, dessen Ordnung gleich $p^{m_1 + m_2 + m_3 + \cdots}$ ist.

Dieser Zusatz geht aus dem vorhergehenden Lehrsatze hervor, wenn darin $n_1 = n_2 = n_3 = \cdots = p$ vorausgesetzt wird. Da die Ordnung des conjugirten Systems eine Potenz von p ist, so hat auch jede Substitution des Systems eine Potenz von p zur Ordnung und ist folglich primitiv.

Zusatz II. — Es ist ein System von n Buchstaben gegeben, und es seien p eine Primzahl, die gleich n oder kleiner als n ist, ν das grösste in n enthaltene Vielfache von p und p^μ die höchste in das Produkt $N = 1.2.3\ldots n$ aufgehende Potenz von p. Dann kann man aus ν beliebig gewählten Buchstaben stets ein System primitiver und conjugirter Substitutionen bilden, dessen Ordnung gleich p^μ ist.

Dieser Zusatz ergiebt sich aus dem vorhergehenden, wenn man voraussetzt, dass $m_1 p$ das grösste in n enthaltene Vielfache von p, $m_2 p$ das grösste in m_1 enthaltene Vielfache von p sei, u. s. w. Unter dieser Voraussetzung ist die Summe

$$\mu = m_1 + m_2 + m_3 + \cdots$$

offenbar der Exponent der höchsten in das Produkt $N = 1.2.3\ldots n$ aufgehenden Potenz von p.

426. Beispiel. — Wir betrachten den Fall, in welchem $n = 6$ ist, und nehmen $p = 2$ an. Die höchste Potenz von 2, welche in 1.2.3.4.5.6 aufgeht, ist 2^4 oder 16; man kann daher aus sechs Buchstaben ein System von sechszehn primitiven und conjugirten Substitutionen bilden. Sind a, b, c, d, e, f die gegebenen Buchstaben, so kann man für die Substitutionen P folgende wählen:

$$(a, b), (c, d), (e, f).$$

Die Reihe der Substitutionen Q reducirt sich hier auf eine einzige Substitution, und man kann

$$(a, c)\ (b, d)$$

nehmen. Das Produkt der vier Systeme

$$\begin{array}{l} 1, (a, b) \\ 1, (c, d) \\ 1, (e, f) \\ 1, (a, c)\ (b, d) \end{array}$$

liefert sechszehn conjugirte Substitutionen, unter denen sich ausser der Einheit folgende befinden:

1⁰ drei Transpositionen, nämlich:

$$(a, b), (c, d), (e, f);$$

2⁰ fünf regelmässige Substitutionen, deren jede aus zwei Transpositionen besteht, nämlich:

$$(a, b)(c, d), (a, b)(e, f), (c, d)(e, f),$$
$$(a, c)(b, d), (a, d)(b, c);$$

3⁰ drei regelmässige Substitutionen, deren jede aus drei Transpositionen besteht, nämlich:

$$(a, b)(c, d)(e, f), (a, c)(b, d)(e, f), (a, d)(b, c)(e, f);$$

4⁰ zwei cyclische Substitutionen vierter Ordnung, nämlich:

$$(a, d, b, c), (a, c, b, d);$$

5⁰ zwei unregelmässige primitive Substitutionen vierter Ordnung, nämlich:

$$(a, d, b, c)(e, f), (a, c, b, d)(e, f).$$

427. Lehrsatz VIII. — Hat man aus m Buchstaben ein conjugirtes System μ^{ter} Ordnung und aus p Buchstaben ein conjugirtes System der Ordnung ω gebildet, so kann man aus $n = mp$ Buchstaben ein System conjugirter Substitutionen construiren, dessen Ordnung gleich $\mu^p \omega$ ist.

Wir vertheilen die mp gegebenen Buchstaben in p Gruppen, deren jede m Buchstaben enthält, und die wir durch

$$\begin{array}{l} a_0, a_1, a_2, \ldots, a_{m-1}, \\ b_0, b_1, b_2, \ldots, b_{m-1}, \\ \ldots\ldots\ldots\ldots, \\ k_0, k_1, k_2, \ldots, k_{m-1} \end{array}$$

darstellen. Es sei nun A ein System von μ conjugirten Substitutionen, welche aus den m Buchstaben a der ersten Reihe dieser Tabelle gebildet sind. Ferner seien $B, C, \ldots, K$ die Systeme conjugirter Substitutionen, welche entstehen, wenn man in A den Buchstaben a der Reihe nach durch $b, c, \ldots, k$ ersetzt, ohne die Indices zu verändern. Endlich bezeichnen wir mit

$$1, S_i, T_i, \ldots, U_i$$

ω conjugirte Substitutionen, welche aus den p Buchstaben

$$a_i\ ,\ b_i\ ,\ \ldots\ ,\ k_i$$

gebildet sind, setzen

$$S = S_0\, S_1 \ldots S_{m-1}\ ,\ T = T_0\, T_1 \ldots T_{m-1}\ ,\ \ldots$$

und nennen P das conjugirte System der Ordnung ω

$$1\ ,\ S\ ,\ T\ ,\ \ldots\ ,\ U,$$

dessen Substitutionen die Wirkung haben, die Horizontalreihen unserer Tabelle gegeneinander zu vertauschen.

Offenbar sind die Systeme A, B, ..., K gegeneinander vertauschbar, und es ist leicht einzusehen, dass ihr Produkt gegen das System P vertauschbar ist. Es seien nämlich A eine Substitution des Systems A und S eine Substitution von P. Die Substitution A, welche zuerst ausgeführt werden möge, versetzt die Buchstaben a und ersetzt die erste Horizontalreihe der Tabelle durch

$$a_0'\ ,\ a_1'\ ,\ a_2'\ ,\ \ldots\ ,\ a'_{m-1}\ ;$$

sodann versetzt die Substitution S die Horizontalreihen der Tabelle; wenn sie die Buchstaben b an die Stelle der a bringen soll, so wird die vorhergehende Reihe durch

$$b_0'\ ,\ b_1'\ ,\ b_2'\ ,\ \ldots\ ,\ b'_{m-1}$$

ersetzt, und zur Beseitigung der Accente genügt die Anwendung der Substitution B^{-1}, wenn B das bezeichnet, was aus A wird, sobald man darin a durch b ersetzt. Man hat danach

$$B^{-1}\, P A = P\ ,\ \text{folglich}\ PA = BP.$$

Daraus geht offenbar hervor, dass man durch Multiplication der $p+1$ Systeme A, B, C, ..., K und P ein conjugirtes System der Ordnung $\mu^p . \omega$ erhält.

Zusatz I. — Aus $n = mp$ Buchstaben lässt sich ein System conjugirter Substitutionen der Ordnung

$$(1.2.3\ldots m)^p\ (1.2.3\ldots p)$$

bilden.

In der That genügt es, für A das System aller aus m und für P das System aller aus p Buchstaben möglichen Substitutionen zu nehmen.

Beispiele. — Wenn $n = 6$ ist, so kann man $m = 3$, $p = 2$, oder $m = 2$, $p = 3$ machen. Man sieht sodann, dass sich aus sechs Buchstaben zwei conjugirte Systeme bilden lassen, deren

Ordnungen beziehungsweise 72 und 48 sind. Für $n = 4$ hat man $m = 2$, $p = 2$, und man erhält aus vier Buchstaben ein conjugirtes System 8ter Ordnung.

Zusatz II. — Wenn p eine Primzahl ist, so kann man aus $n = mp$ Buchstaben ein System conjugirter Substitutionen der Ordnung $(1.2.3\ldots m)^p.p.(p-1)$ bilden.

Es genügt nämlich, A ganz wie in dem vorhergehenden Zusatze zu wählen, und für P das conjugirte System der Ordnung $p(p-1)$ zu nehmen, von dessen Existenz wir uns für den Fall, dass p eine Primzahl ist, überzeugt haben. Das System, um welches es sich hier handelt, werden wir in der Theorie der Gleichungen antreffen.

428. Lehrsatz IX. — Wenn ein auf n Buchstaben bezügliches System conjugirter Substitutionen alle cyclischen Substitutionen dritter Ordnung, die man aus $n-1$ der gegebenen Buchstaben bilden kann, und ausserdem noch andere Substitutionen enthält, so umfasst es alle cyclischen Substitutionen dritter Ordnung, die sich aus den n Buchstaben bilden lassen.

Es seien

$$a_0\,,\ a_1\,,\ a_2\,,\ \ldots\,,\ a_{n-2}\,,\ b$$

die n gegebenen Buchstaben, G das System, welches wir betrachten und G' das conjugirte System, welches aus denjenigen der Substitutionen von G gebildet ist, die b nicht enthalten. Wir bezeichnen mit T eine Substitution von G, welche G' nicht angehört, und setzen voraus, T bringe b, a_i, a_j an die Stelle von a_0, a_1, a_2; i und j sind irgend zwei Indices, welche auch die Werthe 1 und 2 haben können. Da die Substitution $U = (a_0, a_1, a_2)$ der Voraussetzung nach G angehört, so ist dasselbe mit $TUT^{-1} = (b\,, a_i\,, a_j)$ der Fall. Das System G enthält somit alle aus den n Buchstaben gebildeten cyclischen Substitutionen dritter Ordnung.

Zusatz. — Wenn ein auf n Buchstaben bezügliches System conjugirter Substitutionen alle $1.2.3\ldots(n-1) = \frac{N}{n}$ aus $n-1$ Buchstaben gebildeten Substitutionen enthält, so ist seine Ordnung N oder $\frac{N}{n}\cdot$ Enthält das

vorgelegte System nur die $\frac{N}{2n}$ Substitutionen erster Art, die sich aus $n-1$ Buchstaben bilden lassen, so ist seine Ordnung $\frac{N}{2}$ oder $\frac{N}{2n}$.

Wir behalten die im vorhergehenden Lehrsatze angewandten Bezeichnungen bei. Der Voraussetzung nach ist G' von der Ordnung $\frac{N}{n}$ oder $\frac{N}{2n}$; dieselbe Zahl drückt daher auch die Ordnung von G aus, wenn dieses letztere System nur die Substitutionen von G' enthält. Im entgegengesetzten Falle umfasst G alle aus den n Buchstaben möglichen cyclischen Substitutionen dritter Ordnung, und seine Ordnung ist N oder $\frac{N}{2}$, nämlich: N, wenn G' alle Substitutionen der $n-1$ Buchstaben, $\frac{N}{2}$, wenn G' nur Substitutionen erster Art enthält.

429. Lehrsatz X. — Wenn ein auf n Buchstaben bezügliches System conjugirter Substitutionen nicht alle aus $n-1$ Buchstaben gebildeten cyclischen Substitutionen dritter Ordnung, aber alle Substitutionen dieser Art enthält, die sich aus $n-2$ der gegebenen Buchstaben bilden lassen, so können diejenigen seiner Substitutionen, welche die beiden andern Buchstaben versetzen, dieselben nur gegeneinander vertauschen. Es wird dabei vorausgesetzt, dass die Zahl n grösser als 4 sei.

Es seien

$$a_0, a_1, a_2, \ldots, a_{n-3}, b_0, b_1$$

die n gegebenen Buchstaben, G das System, welches man betrachtet, und G' das conjugirte System, welches aus denjenigen der Substitutionen von G zusammengesetzt ist, die keinen der Buchstaben b_0, b_1 versetzen. Der Voraussetzung nach enthält G alle cyclischen Substitutionen dritter Ordnung, die man aus den $n-2$ Buchstaben a bilden kann. Wir bezeichnen mit T eine Substitution des Systems G, welche G' nicht angehört, und welche die Buchstaben b_0 und b_1 nicht gegeneinander vertauscht.

Wenn die Substitution T den Buchstaben b_0 versetzt, um ihn an die Stelle von a_0 zu bringen, während b_1 seinen Platz beibehält, oder wenn sie b_1 auf den Platz von b_0 bringt, so

mögen a_1 und a_2 die beiden Buchstaben sein, welche durch irgend zwei gegebene Buchstaben a_i, a_j ersetzt werden. Da die Substitution $U = (a_0, a_1, a_2)$ dem Systeme G angehört, so ist dasselbe mit $TUT^{-1} = (b_0, a_i, a_j)$ der Fall; folglich enthält G alle cyclischen Substitutionen dritter Ordnung, die sich aus $n-1$ der gegebenen Buchstaben bilden lassen, was der Voraussetzung widerspricht.

Wenn T die Buchstaben b_0, b_1, a_i auf die Plätze von a_0, a_1, a_2 bringt, so muss, da $U = (a_0, a_1, a_2)$ dem Systeme G angehört, auch $TUT^{-1} = (b_0, b_1, a_i)$ eine Substitution dieses Systems sein. Letztere ersetzt nun a_i durch b_0 und b_0 durch b_1; wir gelangen somit wieder zum vorigen Falle, der, wie wir so eben gesehen haben, mit der Voraussetzung im Widerspruch steht.

Es ergiebt sich also, dass die Substitution T die Buchstaben b_0, b_1 nur gegeneinander vertauschen kann; sie ist folglich von der Form $T = (b_0, b_1) S$, wo S eine Substitution von G' ist. Man sieht zugleich, dass das System G dadurch erhalten wird, dass man das System G' und das aus den beiden Substitutionen $1, (b_0, b_1)$ bestehende System miteinander multiplicirt. Die Ordnung von G ist daher doppelt so gross, als diejenige von G'.

Anmerkung. — Der vorhergehende Beweis erfordert, dass die Anzahl der Buchstaben a wenigstens gleich 3, dass also $n > 4$ sei. Für $n = 4$ bleibt der Satz nicht bestehen.

Zusatz. — Wenn ein auf n Buchstaben bezügliches System conjugirter Substitutionen alle

$$1.2.3\ldots(n-2) = \frac{N}{n(n-1)}$$

aus $n-2$ der gegebenen Buchstaben gebildeten, aber nicht alle Substitutionen enthält, die man aus $n-1$ Buchstaben bilden kann, so ist seine Ordnung gleich dem Quotienten der Division von N durch eine der beiden Zahlen $\frac{n(n-1)}{2}$, $n(n-1)$. Wenn das System nur die $\frac{N}{2n(n-1)}$ Substitutionen erster Art umfasst, die sich aus $n-2$ Buchstaben zusammensetzen lassen, aber nicht alle Substitutionen erster Art, die aus $n-1$ Buchstaben möglich sind, so ist seine Ordnung gleich dem Quotienten der Division von N durch eine der beiden Zahlen $n(n-1)$, $2n(n-1)$.

Der Voraussetzung nach hat G' die Ordnung $\frac{N}{n(n-1)}$ oder $\frac{N}{2n(n-1)}$. Dieselbe Zahl drückt die Ordnung von G aus, wenn dieses System nur die Substitutionen von G' enthält. Im entgegengesetzten Falle hat jede Substitution von G, die G' nicht angehört, eine cyclische Versetzung der beiden in G' nicht enthaltenen Buchstaben zur Folge; denn sonst würde G, der Voraussetzung zuwider, alle cyclischen Substitutionen dritter Ordnung umfassen, die aus $n-1$ Buchstaben gebildet werden können. Nach dem vorhergehenden Lehrsatze ist dann die Ordnung von G doppelt so gross, als diejenige von G'.

Permutations-Gruppen.

430. Wir betrachten ein System Γ conjugirter Substitutionen, dessen Ordnung gleich μ sein möge; die aus n Buchstaben gebildeten Substitutionen dieses Systems seien

$$1, S_1, S_2, \ldots, S_{\mu-1}.$$

Nimmt man irgend eine Permutation A_0 der n gegebenen Buchstaben und multiplicirt dieselbe mit den μ Substitutionen von Γ, so erhält man μ Produkte

$$A_0, S_1 A_0, S_2 A_0, \ldots, S_{\mu-1} A_0,$$

oder

$$A_0, A_1, A_2, \ldots, A_{\mu-1},$$

welche eine Gruppe von Permutationen ausmachen. Die Substitutionen des Systems Γ, mittels welcher man von einer Permutation zu einer anderen übergeht, heissen die Substitutionen der Gruppe.

Wir bezeichnen mit G das System der $N = 1.2.3\ldots n$ Substitutionen der gegebenen Buchstaben, oder auch irgend ein anderes conjugirte System, welches alle Substitutionen des Systems Γ enthält. Ist $m = \mu q$ die Ordnung von G, so können die Substitutionen dieses Systems nach No. 413 auf jede der beiden folgenden Arten dargestellt werden:

$$(1). \quad \begin{cases} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ T_1, & S_1 T_1, & S_2 T_1, & \ldots, & S_{\mu-1} T_1, \\ T_2, & S_1 T_2, & S_2 T_2, & \ldots, & S_{\mu-1} T_2, \\ \cdot & \cdot & \cdot & \cdot & \cdot \quad, \\ T_{q-1}, & S_1 T_{q-1}, & S_2 T_{q-1}, & \ldots, & S_{\mu-1} T_{q-1}; \end{cases}$$

$$(2). \quad \begin{cases} 1 \quad , S_1 \quad , S_2 \quad , \ldots , S_{\mu-1} \quad , \\ U_1 \quad , U_1 S_1 \quad , U_1 S_2 \quad , \ldots , U_1 S_{\mu-1} \quad , \\ U_2 \quad , U_2 S_1 \quad , U_2 S_2 \quad , \ldots , U_2 S_{\mu-1} \quad , \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad , \\ U_{q-1} , U_{q-1} S_1 , U_{q-1} S_2 , \ldots , U_{q-1} S_{\mu-1} . \end{cases}$$

Dies vorausgesetzt, erhält man eine Gruppe von m Permutationen, wenn man die nach Belieben gewählte Permutation A_0 mit den m Substitutionen von G multiplicirt, und zur Ausführung dieser Operation kann man jede der Formen (1) und (2) von G benutzen.

Wir wollen zunächst die Form (1) in Anwendung bringen. Die erste Horizontalreihe besteht aus den μ Substitutionen des Systems Γ, und durch Multiplication der Permutation A_0 mit diesen Substitutionen entsteht die bereits oben betrachtete Gruppe, nämlich

$$A_0 , A_1 , A_2 , \ldots , A_{\mu-1}.$$

Um A_0 mit den Substitutionen der zweiten Reihe der Tabelle (1) zu multipliciren, genügt es, das Produkt $A_0^{(1)}$ der Permutation A_0 in T_1 zu bilden, und dieses Produkt sodann mit den Substitutionen Γ zu multipliciren. Die Resultate

$$A_0^{(1)} , A_1^{(1)} , A_2^{(1)} , \ldots , A_{\mu-1}^{(1)} ,$$

die man auf diese Weise erhält, bilden offenbar eine zweite Permutations-Gruppe, welche dieselben Substitutionen, wie die vorhergehende, zulässt.

Die vorstehende Betrachtung lässt sich offenbar auch für die übrigen Reihen der Tabelle (1) anstellen, und wir erhalten somit folgendes Resultat:

Die durch Multiplication einer Permutation A_0 mit den μq Substitutionen des Systems G erhaltene Gruppe von Permutationen lässt sich in q Gruppen zerlegen, deren jede aus μ Permutationen besteht, und diese verschiedenen partiellen Gruppen lassen dieselben Substitutionen, nämlich die des Systems Γ zu.

Ebenso verfahren wir, wenn die Form (2) des Systems G zu benutzen ist. Die erste Reihe der Tabelle (2) liefert gleichfalls die Gruppe

$$A_0 , A_1 , A_2 , \ldots , A_{\mu-1} .$$

Was die folgenden Reihen betrifft, so liefern dieselben als Resul-

tate die Produkte, die man dadurch erhält, dass man diese erste Gruppe der Reihe nach mit den Substitutionen

$$U_1 \ , \ U_2 \ , \ \ldots \ , \ U_{q-1}$$

multiplicirt, und da diese Operationen gleichbedeutend sind mit einfachen Aenderungen in der zur Darstellung der Buchstaben angewandten Bezeichnung, so verwandelt jede von ihnen die erste Gruppe in eine andere Gruppe. Daraus geht Folgendes hervor:

Die durch Multiplication einer Permutation A_0 mit den μq Substitutionen des Systems G erhaltene Gruppe lässt sich in q Gruppen von je μ Permutationen zerlegen; der Uebergang von einer Gruppe zu einer andern erfolgt dadurch, dass man die Permutationen der ersten Gruppe ein und derselben Substitution unterwirft.

Es kann vorkommen, dass die Horizontalreihen in den Tabellen (1) und (2) dieselben sind. Dieser Umstand wird jedenfalls eintreten, wenn die Substitutionen

$$1 \ , \ T_1 \ , \ T_2 \ , \ \ldots \ , \ T_{q-1} \, ,$$

oder

$$1 \ , \ U_1 \ , \ U_2 \ , \ \ldots \ , \ U_{q-1}$$

ein gegen Γ vertauschbares conjugirtes System bilden. In diesem Falle lässt sich die Permutations-Gruppe, die man durch Multiplication der Permutation A_0 mit den μq Substitutionen des Systems G erhält, in q aus je μ Permutationen bestehende Gruppen zerlegen, welche die Doppeleigenschaft besitzen, dass die Substitutionen in den verschiedenen partiellen Gruppen dieselben sind, und dass der Uebergang von einer derselben zu einer andern dadurch erfolgt, dass man ein und dieselbe Substitution an den Permutationen der ersten Gruppe ausführt.

431. Beispiel. — Wir betrachten den Fall von vier Buchstaben a, b, c, d, und nehmen die vier Systeme conjugirter Substitutionen:

$$\begin{aligned} G &= 1 \ , \ (a \, , b) \ (c \, , d) \, , \\ G' &= 1 \ , \ (a \, , c) \ (b \, , d) \, , \\ G'' &= 1 \ , \ (b \, , c \, , d) \ , \ (b \, , d \, , c) \, , \\ G''' &= 1 \ , \ (b \, , c) . \end{aligned}$$

Die Systeme G und G' sind vertauschbar, und ihr Produkt $G'G$ ist ein gegen G'' vertauschbares conjugirtes System vierter Ordnung; das conjugirte System $G''G'G$ endlich ist gegen G''' vertauschbar, so dass das Produkt $G'''G''G'G$ die vierundzwanzig Substitutionen umfasst.

Multipliciren wir, dies vorausgesetzt, die Permutation $abcd$ mit dem System $G'''G''G'G$, so erhalten wir die Gruppe der vierundzwanzig Permutationen:

$abcd$	$acdb$	$adbc$	$acbd$	$abdc$	$adcb$
$badc$	$cabd$	$dacb$	$cadb$	$bacd$	$dabc$
$cdab$	$dbac$	$bcad$	$bdac$	$dcab$	$cbad$
$dcba$	$bdac$	$cbda$	$dbca$	$cdba$	$bcda$

Diese Gruppe zerfällt in zwei andere; die eine derselben umfasst die Permutationen der drei ersten Colonnen und lässt, wie die zweite, die zwölf Substitutionen erster Art zu; der Uebergang von einer dieser partiellen Gruppen zur andern erfolgt durch Ausführung der Transposition (b, c).

Die erste dieser beiden Gruppen zerfällt ihrerseits wieder in drei andere Gruppen, deren jede aus den in ein und derselben Colonne enthaltenen Permutationen besteht; diese drei partiellen Gruppen lassen die vier Substitutionen des Systems $G'G$ zu, und man gelangt von einer zur andern mittels ein und derselben Substitution von G''.

Die erste dieser drei letzten Gruppen endlich lässt sich in zwei andere Gruppen zerlegen, von denen die erste aus den beiden ersten, die zweite aus den beiden letzten Permutationen besteht. Jede dieser partiellen Gruppen lässt die Substitution von G zu, und man gelangt von der einen zur andern durch Ausführung der Substitution von G'.

Drittes Kapitel.

Indices der conjugirten Systeme.

Index eines conjugirten Systems. — Untere Grenze der Indices, die grösser als 2 sind.

432. Um eine kurze Ausdrucksweise zu erhalten, werden wir unter dem Index eines aus n Buchstaben gebildeten Systems conjugirter Substitutionen den Quotienten verstehen, den man erhält, wenn das Produkt $N = 1 . 2 . 3 \ldots n$ durch die Zahl dividirt wird, welche die Ordnung des Systems ausdrückt. Bezeichnet m den Index eines conjugirten Systems μ^{ter} Ordnung, so hat man

$$m = \frac{N}{\mu}.$$

Die Ordnung und der Index eines auf n Buchstaben bezüglichen conjugirten Systems sind daher zwei einander entsprechende Divisoren des Produkts $1 . 2 . 3 \ldots n$.

Welches auch die Anzahl n der Buchstaben sei, der Index m kann stets die Werthe 1 und 2 haben, und es ist von Interesse, allgemein die kleinsten Werthe kennen zu lernen, welche derselbe haben kann, sobald er grösser als 2 ist.

Rufini hat in seiner Theorie der Gleichungen den Fall von fünf Buchstaben besonders erörtert, und aus seinen Untersuchungen lässt sich Folgendes entnehmen: Wenn der Index eines aus fünf Buchstaben gebildeten conjugirten Systems grösser als 2 ist, so ist er wenigstens gleich 5.

Später hat Cauchy im Journal de l'École Polytechnique, Cah. X, einen allgemeineren Satz bewiesen, aus welchem die beiden folgenden Sätze hervorgehen:

Der Index eines auf n Buchstaben bezüglichen conjugirten Systems kann nicht zu gleicher Zeit grösser als 2 und kleiner als die grösste der Primzahlen sein, welche nicht grösser als n sind.

Wenn n eine Primzahl ist, so kann der Index eines aus n Buchstaben gebildeten conjugirten Systems nicht zu gleicher Zeit grösser als 2 und kleiner als n sein.

Den letzten Satz suchte Cauchy, wie er in der erwähnten Arbeit zu verstehen giebt, auch auf den Fall auszudehnen, in welchem n eine zusammengesetzte Zahl ist. Er konnte aber anfangs nur für den Fall $n = 6$ zum Ziele gelangen; in der That bewies er, dass der Index eines aus sechs Buchstaben gebildeten conjugirten Systems nicht gleichzeitig grösser als 2 und kleiner als 6 sein kann.

Dieselbe Frage hat darauf Bertrand mit Erfolg in Angriff genommen, der zuerst den folgenden Satz allgemein bewies:

Der Index eines aus n Buchstaben gebildeten Systems conjugirter Substitutionen kann nicht zu gleiher Zeit grösser als 2 und kleiner als n sein.

Der Beweis, den Bertrand (Journal de l'École Polytechnique, Cahier XXX) giebt, beruht aber auf einem dieser Theorie völlig fremdartigen Postulat und ist von diesem Gesichtspunkte aus nicht ganz genügend. Das in Rede stehende Postulat haben wir in No. 391 bewiesen; es besteht in Folgendem:

Wenn $n > 7$ ist, so liegt wenigstens eine Primzahl zwischen $\frac{n}{2}$ und $n - 2$.

Das von Bertrand angewandte Schlussverfahren führt noch zu dem folgenden Satze, den Abel für den Fall $n = 5$ schon vorher bewiesen hatte:

Wenn der Index eines aus n Buchstaben gebildeten Systems conjugirter Substitutionen gleich n ist, so besteht das System aus den $1 . 2 \ldots (n - 1)$ Substitutionen von $n - 1$ Buchstaben.

In einer im Journal de l'École Polytechnique, Cah. XXXII, enthaltenen Note habe ich gezeigt, dass der Satz von Bertrand, falls zwischen $n - 2$ und $\frac{n}{2}$ keine Primzal enthalten ist, doch

bestehen bleibt, vorausgesetzt dass $\frac{n}{2}$ eine Primzahl ist. Die Richtigkeit dieser Bemerkung ergiebt sich, ohne dass man nöthig hätte, den Beweis des Satzes irgendwie zu modificiren. Nur kann man dann nicht mehr den Zusatz herleiten, nach welchem das conjugirte System aus den $1 . 2 \ldots (n - 1)$ Substitutionen von $n - 1$ Buchstaben besteht, wenn der Index des Systems gleich der Anzahl n der Buchstaben ist.

Diese Bemerkung ist nicht unwichtig; denn sie zeigt, dass der Satz von Cauchy, welcher sich auf den Fall $n = 6$ bezieht, und dessen Beweis ziemlich complicirt ist, sich aus dem Bertrand'schen Satze ohne Weiteres entnehmen lässt. In der That giebt es, wenn $n = 6$ ist, keine Primzahl zwischen $n - 2$ und $\frac{n}{2}$; aber $\frac{n}{2}$ oder 3 ist eine Primzahl.

Bertrand hat in seiner Arbeit auch folgenden Satz bewiesen:

Wenn die Zahl $n > 9$ und der Index eines aus n Buchstaben gebildeten Systems conjugirter Substitutionen grösser als n ist, so ist dieser Index wenigstens gleich $2n$.

Später habe ich in einer 1849 der Akademie vorgelegten Abhandlung (Journal de Mathématiques pures et appliquées, 1re série, t. XV), ohne zu irgend einem Postulat meine Zuflucht zu nehmen, die nachstehenden Lehrsätze hergeleitet:

1°. Der Index eines Systems conjugirter Substitutionen, die aus n Buchstaben gebildet sind, kann nicht zugleich grösser als 2 und kleiner als n sein, wofern nicht $n = 4$ ist.

2°. Wenn der Index eines conjugirten Systems genau gleich der Anzahl n der Buchstaben ist, so besteht das System aus allen Substitutionen von $n - 1$ Buchstaben, wofern nicht $n = 6$ ist.

3°. Wenn der Index eines conjugirten Systems grösser als die Anzahl n der Buchstaben ist, so ist er wenigstens gleich $2n$, vorausgesetzt dass $n > 8$ ist.

4°. Wenn der Index eines auf n Buchstaben bezüglichen conjugirten Systems grösser als $2n$ ist, so

ist er wenigstens gleich $\frac{n(n-1)}{2}$, vorausgesetzt dass $n > 12$ ist.

Die Beweise, die ich für diese Sätze gegeben habe, lassen hinsichtlich der Strenge Nichts zu wünschen übrig. Cauchy hatte die Frage gleichfalls wieder aufgenommen und andere Beweise eben derselben Sätze gefunden. Diese Beweise beruhen auf neuen Begriffen, welche für die Theorie, mit der wir uns jetzt beschäftigen, von grosser Bedeutung sind, und die wir daher nicht unerörtert lassen können. Wir halten es aber für zweckmässig, zunächst die Betrachtungen vorzuführen, die Cauchy in seiner ersten Arbeit zur Herleitung des ersten der beiden oben angegebenen Sätze angestellt hat. Auch können wir die geistreiche und elegante Untersuchung, durch welche Bertrand zum Beweise seines Satzes gelangt, nicht mit Stillschweigen übergehen.

433. Satz von Cauchy. — Der Index eines Systems conjugirter Substitutionen, die aus n Buchstaben gebildet sind, kann nicht zu gleicher Zeit grösser als 2 und kleiner als die grösste der Primzahlen sein, die nicht grösser als n sind.

Die aus n Buchstaben gebildeten Substitutionen eines conjugirten Systems μ^{ter} Ordnung G seien

$$1\,,\ S_1\,,\ S_2\,,\ S_3\,,\ \ldots\,,\ S_{\mu-1}\,.$$

Multiplicirt man dieselben, etwa zur Linken, mit den verschiedenen Potenzen irgend einer cyclischen Substitution T, deren Ordnung p eine Primzahl und gleich n oder kleiner als n ist, so erhält man die folgende aus μp Substitutionen bestehende Tabelle:

$$\begin{array}{llllll}
1\,, & S_1\,, & S_2\,, & \ldots\,, & S_{\mu-1}\,, \\
T\,, & TS_1\,, & TS_2\,, & \ldots\,, & TS_{\mu-1}\,, \\
T^2\,, & T^2S_1\,, & T^2S_2\,, & \ldots\,, & T^2S_{\mu-1}\,, \\
. & . & . & . & . \,, \\
T^{p-1}, & T^{p-1}S_1, & T^{p-1}S_2, & \ldots\,, & T^{p-1}S_{\mu-1}\,.
\end{array}$$

Wenn der Index $\frac{N}{\mu}$ des Systems G kleiner als p ist, so hat man $\mu p > N$, und es werden folglich in der vorstehenden Tabelle zwei gleiche Substitutionen anzutreffen sein. Es sei

$$T^\alpha S_i = T^\beta S_j;$$

die Exponenten α und β müssen als ungleich vorausgesetzt werden; denn hätte man $\beta = \alpha$, so würde $S_j = S_i$ oder $j = i$ sein. Aus der vorhergehenden Relation ergiebt sich

$$T^{\alpha-\beta} = S_j S_i^{-1} \text{ oder } T^\gamma = S_j S_i^{-1}.$$

Da das Produkt $S_j S_i^{-1}$ eine von 1 verschiedene Substitution des Systems G ist, so sieht man, dass dieses System eine Potenz T^γ von T enthalten muss; es enthält daher alle Potenzen von T^γ. Nun ist aber die Ordnung der cyclischen Substitution T eine Primzahl; T findet sich somit in der Reihe der Potenzen von T^γ vor und gehört folglich dem Systeme G an.

Danach enthält das System G alle cyclischen Substitutionen p^{ter} Ordnung; es umfasst mithin (No. 418) N oder $\frac{N}{2}$ Substitutionen, d. h. sein Index ist gleich 1 oder gleich 2.

434. Satz von Bertrand. — Der Index eines Systems conjugirter Substitutionen, die aus n Buchstaben gebildet sind, kann nicht zu gleicher Zeit grösser als 2 und kleiner als n sein.

Wie wir schon bemerkt haben, setzt Bertrand voraus, dass zwischen $\frac{n}{2}$ und $n - 2$ wenigstens eine Primzahl liegt, wenn $n > 7$ ist.

Wir betrachten das System G der conjugirten Substitutionen

$$1, S_1, S_2, \ldots, S_{\mu-1},$$

die aus n Buchstaben gebildet sind, und nehmen an, der Index $\frac{N}{\mu}$ dieses Systems sei kleiner als n. Ferner bezeichnen wir mit p eine zwischen $\frac{n}{2}$ und $n - 2$ enthaltene Primzahl, nehmen irgend welche $p + 2$ der n gegebenen Buchstaben und bilden aus p dieser $p + 2$ Buchstaben eine cyclische Substitution p^{ter} Ordnung T, aus den beiden übrig bleibenden Buchstaben eine Transposition U. Dies vorausgesetzt, multipliciren wir die Substitutionen des Systems G, etwa zur Linken, mit den p Potenzen von T, die erhaltenen Produkte sodann mit den beiden Potenzen von U. Auf diese Weise erhalten wir die beiden folgenden Tabellen:

$$\begin{cases} 1 &, S_1 &, S_2 &, \ldots, & S_{\mu-1}, \\ T &, TS_1 &, TS_2 &, \ldots, & TS_{\mu-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ T^{p-1} &, T^{p-1}S_1 &, T^{p-1}S_2 &, \ldots, & T^{p-1}S_{\mu-1}, \end{cases}$$

$$\begin{cases} U &, US_1 &, US_2 &, \ldots, & US_{\mu-1}, \\ UT &, UTS_1 &, UTS_2 &, \ldots, & UTS_{\mu-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ UT^{p-1} &, UT^{p-1}S_1 &, UT^{p-1}S_2 &, \ldots, & UT^{p-1}S_{\mu-1}, \end{cases}$$

in welchen sich $2p\mu$ Substitutionen vorfinden. Der Voraussetzung nach ist aber p wenigstens gleich $\frac{n}{2}$ und μ grösser als $\frac{N}{n}$; folglich ist die Anzahl unserer Substitutionen grösser als N, und es müssen zwei derselben einander gleich sein.

Wenn diese beiden gleichen Substitutionen derselben Tabelle angehören, so hat man etwa

$$T^\alpha S_i = T^\beta S_j \text{ oder } UT^\alpha S_i = UT^\beta S_j,$$

wo α und β zwei ungleiche Exponenten bezeichnen, und daraus folgt

$$T^{\alpha-\beta} = S_j S_i^{-1}.$$

Die Substitution $T^{\alpha-\beta}$ gehört also dem Systeme G an, und man folgert weiter, wie im vorhergehenden Satze, dass auch T eine Substitution dieses Systems ist.

Wenn die beiden gleichen Substitutionen nicht derselben Tabelle angehören, so hat man

$$T^\alpha S_i = UT^\beta S_j = T^\beta U S_j;$$

denn die Reihenfolge der Substitutionen U und T, die keinen Buchstaben gemeinschaftlich haben, lässt sich umkehren. Aus dieser Gleichung ergiebt sich, mit Rücksicht auf die Relation $U^{-1} = U$,

$$T^{\alpha-\beta} U = S_j S_i^{-1};$$

daraus geht hervor, dass die Substitution $T^{\alpha-\beta}U$, folglich auch ihr Quadrat

$$T^{2\alpha-2\beta}U^2 = T^{2\alpha-2\beta}$$

dem Systeme G angehört. Die Differenz $\alpha - \beta$ kann Null sein; dann gehört die Substitution U dem Systeme G an. Ist aber $\alpha - \beta$

von Null verschieden, so gehört $T^{2(\alpha-\beta)}$ zum Systeme G und ebenso alle Potenzen dieser Substitution, unter denen sich, wie bei der vorigen Voraussetzung, auch T befindet. In diesem letzten Falle gehören T und $T^{\alpha-\beta}U$, folglich auch U dem Systeme G angehört.

Wir sehen somit, dass wenigstens eine der beiden Substitutionen T und U dem Systeme G angehört.

Wir nehmen jetzt an, der Index des vorgelegten Systems reducire sich nicht auf 1, oder die Ordnung dieses Systems sei nicht gleich N. Dann ist wenigstens eine der Transpositionen, die man aus den n gegebenen Buchstaben bilden kann, unter den Substitutionen von G nicht enthalten. Diese Transposition nehmen wir für U, so dass nach dem Vorhergehenden jede cyclische Substitution p^{ter} Ordnung T, welche aus den $n-2$ in U nicht enthaltenen Buchstaben gebildet ist, dem Systeme G angehört. Diejenigen der Substitutionen von G, welche die beiden Buchstaben der Transposition U nicht versetzen, bilden offenbar ein conjugirtes System G', und da G' alle cyclischen Substitutionen p^{ter} Ordnung umfasst, so ist seine Ordnung gleich $1.2.3\ldots(n-2)$ oder gleich der Hälfte dieser Zahl (No. 418). Der erste dieser beiden Fälle kann jedoch nicht stattfinden; denn sonst müsste der Index von G, welcher grösser als 1 ist, wenigstens gleich n sein (No. 429, Zusatz), was der Voraussetzung widerspricht. Die Ordnung von G' ist daher $\frac{1.2\ldots(n-2)}{2}$, und folglich ist der Index dieses Systems gleich 2.

Das System G' enthält danach nur Substitutionen erster Art, und folglich umfasst das System G keine der Transpositionen, die man aus den auf G' bezüglichen Buchstaben bilden kann. Wir bezeichnen mit U' irgend eine dieser Transpositionen und mit T' eine cyclische Substitution p^{ter} Ordnung, welche keinen Buchstaben von U', aber wenigstens einen der beiden Buchstaben von U enthält. Da die Transposition U' sich in G nicht vorfindet, so gehört, wie wir oben gesehen haben, T' diesem Systeme an, woraus hervorgeht, dass G alle cyclischen Substitutionen p^{ter} Ordnung enthält, die sich aus den n gegebenen Buchstaben zusammensetzen lassen. Das System G umfasst daher alle aus diesen Buchstaben möglichen Substitutionen erster Art. Ausserdem ist es klar, dass G keine anderen Substitutionen enthalten

kann; denn es fehlen ihm die Substitutionen zweiter Art, welche aus den $n - 2$ auf G' bezüglichen Buchstaben gebildet sind; die Ordnung dieses Systems ist daher gleich $\frac{N}{2}$, und sein Index ist gleich 2*).

435. Die vorstehenden Schlüsse gelten auch noch, wenn zwischen $\frac{n}{2}$ und $n - 2$ keine Primzahl liegt, vorausgesetzt dass $\frac{n}{2}$ eine Primzahl ist. Man kann dann $p = \frac{n}{2}$ setzen; von dieser Art ist der Fall $n = 6$. Wenn aber zwischen $\frac{n}{2}$ und $n - 2$ wirklich eine Primzahl enthalten ist, so kann das oben dargelegte Schlussverfahren noch zum Beweise eines neuen sehr wichtigen Satzes benutzt werden. Um nämlich zu zeigen, dass das System G wenigstens eine der Substitutionen T und U enthält, ist die oben gemachte Voraussetzung, dass der Index von G kleiner als n sei, nicht erforderlich; dasselbe findet noch statt, wenn dieser Index gleich n ist, vorausgesetzt dass man $p > \frac{n}{2}$ hat, und man gelangt immer zu dem Ergebniss, dass der Index von G' 1 oder 2 ist. Dieser Index kann nicht gleich 2 sein; denn aus dieser Annahme würde sich, wie wir gesehen haben, ergeben, dass auch G den Index 2 hat, was der Voraussetzung widerspricht. Der Index von G' ist daher gleich 1; dann kann aber (No. 429, Zusatz) der Index von G nicht gleich n sein, wofern dieses System nicht durch die Substitutionen von $n - 1$ Buchstaben gebildet wird. Wir erhalten auf diese Weise den folgenden Satz:

Lehrsatz. — Wenn der Index eines Systems conjugirter Substitutionen gleich der Anzahl n der Buchstaben ist, so besteht das System aus den $1.2.3\ldots(n-1)$ Substitutionen, die aus $n - 1$ Buchstaben gebildet werden können.

Der Beweis bezieht sich nicht auf die Fälle $n = 3, 4, 5, 6, 7$. Für $n = 5$ ist der Satz von Abel bewiesen (Oeuvres complètes, t. I, p. 19). Wie wir später sehen werden, findet er auch für

*) Man hätte diesen Schluss unmittelbar aus den in No. 428 u. 429 hergeleiteten Sätzen ziehen können; wir haben aber vorgezogen, das von Bertrand angewandte Schlussverfahren unverändert wiederzugeben.

$n = 4, 5, 7$ statt. Nur der Fall $n = 6$ macht eine Ausnahme; wir werden zeigen, dass es in der That ein auf 6 Buchstaben bezügliches System conjugirter Substitutionen giebt, dessen Index gleich 6 ist, und welches cyclische Substitutionen der Ordnungen 4, 5, 6 enthält.

Neuer Beweis des Satzes über die untere Grenze der Indices, die grösser als 2 sind.

436. Ich werde jetzt die Betrachtung darlegen, durch welche es mir gelungen ist, den Satz von Bertrand direkt zu beweisen. Dieselbe ist zum ersten Male im Journal de Mathématiques pures et appliquées, I. série, T. XV, veröffentlicht und später in der vorigen Auflage dieses Werkes nochmals mitgetheilt worden. In der folgenden Darstellung werde ich mich der im vorigen Kapitel bewiesenen Sätze bedienen, und dadurch wird es möglich sein, die Sache etwas zu vereinfachen. Der Beweis, um den es sich handelt, wird sich auf zwei Hilfssätze stützen, die ich zunächst herzuleiten habe.

Hilfssatz I. — Es seien G ein System conjugirter Substitutionen, welche aus den n Buchstaben $a_0, a_1, a_2, \ldots, a_{n-3}, b_0, b_1$ gebildet sind, und G' das conjugirte System, welches aus denjenigen der Substitutionen von G besteht, die keinen der beiden Buchstaben b_0, b_1 versetzen. Wenn die Systeme G und G' ein und denselben Index $\mu > 1$ haben, so kann man aus den $n-2$ Buchstaben $a_0, a_1, \ldots, a_{n-3}$ ein System conjugirter Substitutionen zusammensetzen, dessen Index gleich $\frac{\mu}{2}$ ist. Daraus geht hervor, dass μ stets eine gerade Zahl ist.

Wir bezeichnen mit ν und ϱ beziehungsweise die Ordnungen der Systeme G und G'. Dann sind die Indices dieser Systeme $\frac{1 \cdot 2 \cdot 3 \ldots n}{\nu}$ und $\frac{1 \cdot 2 \cdot 3 \ldots (n-2)}{\varrho}$. Da diese Indices der Voraussetzung nach einander gleich sind, so hat man

$$\nu = n(n-1)\varrho.$$

Wir setzen

$$G = 1, S_1, S_2, S_3, \ldots, S_{\varrho-1}, \ldots, S_{\nu-1},$$
$$G' = 1, S_1, S_2, S_3, \ldots, S_{\varrho-1}.$$

Stellt man durch T_1, T_2, ..., $T_{\mu-1}$ Substitutionen der $n-2$ Buchstaben a dar, so kann das System der $\mu\varrho = 1 . 2 . 3 \ldots (n-2)$ Substitutionen der $n-2$ Buchstaben a nach No. 413 in folgender Weise dargestellt werden:

$$(1). \quad \begin{cases} 1 \quad , S_1 \quad , S_2 \quad , \ldots, S_{\varrho-1}, \\ T_1 \quad , T_1 S_1 \quad , T_1 S_2 \quad , \ldots, T_1 S_{\varrho-1}, \\ T_2 \quad , T_2 S_1 \quad , T_2 S_2 \quad , \ldots, T_2 S_{\varrho-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ T_{\mu-1}, T_{\mu-1} S_1, T_{\mu-1} S_2, \ldots, T_{\mu-1} S_{\varrho-1}, \end{cases}$$

und ich behaupte, dass das System der $\mu\nu = 1 . 2 \ldots n$ Substitutionen der n Buchstaben in der neuen Tabelle

$$(2). \quad \begin{cases} 1 \quad , S_1 \quad , S_2 \quad , \ldots, S_{\nu-1}, \\ T_1 \quad , T_1 S_1 \quad , T_1 S_2 \quad , \ldots, T_1 S_{\nu-1}, \\ T_2 \quad , T_2 S_1 \quad , T_2 S_2 \quad , \ldots, T_2 S_{\nu-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ T_{\mu-1}, T_{\mu-1} S_1, T_{\mu-1} S_2, \ldots, T_{\mu-1} S_{\nu-1} \end{cases}$$

enthalten ist, in welcher die Substitutionen T dieselben, wie in der Tabelle (1) sind. Es genügt zu beweisen, dass diese $\mu\nu$ Substitutionen von einander verschieden sind. Hätte man

$$T_i S_j = T_{i'} S_{j'},$$

so würde daraus

$$T_{i'} = T_i S_j S_{j'}^{-1}$$

folgen. Nun sind die Factoren T von b_0 und b_1 unabhängig; mithin enthält auch das Produkt $S_j S_{j'}^{-1}$, welches eine der Substitutionen S_k des Systems G ist, die Buchstaben b_0 und b_1 nicht; daraus geht hervor, dass S_k eine Substitution des Systems G' ist. Ausserdem geht die vorhergehende Gleichung über in

$$T_{i'} = T_i S_k,$$

was nach der Art und Weise, wie die Substitutionen T gewählt sind, um die Tabelle (1) zu bilden, unmöglich der Fall sein kann.

Die Tabelle (2) enthält daher alle Substitutionen der n Buchstaben. Wendet man diese Substitutionen auf irgend eine Permutation an, so werden augenscheinlich $1 . 2 . 3 \ldots (n-2)$ derselben irgend zwei gegebene Buchstaben auf zwei bestimmte Plätze bringen. Da überdies die Substitutionen T die Buchstaben

b_0 und b_1 nicht enthalten, so leuchtet ein, dass alle in ein und derselben Verticalreihe der Tabelle (2) enthaltenen μ Substitutionen b_0 und b_1 dieselben Plätze anweisen. Es giebt daher in der ersten Horizontalreihe der Tabelle, d. h. in dem Systeme G, $\frac{1 . 2 . 3 \ldots (n-2)}{\mu}$ oder ϱ Substitutionen, welche b_0 und b_1 auf irgend zwei Plätze bringen, und welche folglich diese Buchstaben in der Permutation, die man zu Grunde gelegt hat, auf die Plätze von irgend zwei Buchstaben setzen, unter welchen letzteren auch b_0 und b_1 selbst sich vorfinden können. Im Besonderen giebt es genau ϱ Substitutionen, welche b_0 und b_1 gegen einander vertauschen. Setzt man

$$U = (b_0 \, , b_1) \, ,$$

so sind diese ϱ Substitutionen von der Form

$$US_0' \, , \; US_1' \, , \; US_2' \, , \; \ldots \, , \; US_{\varrho-1}' \, ,$$

wo S_0', S_1', ..., $S_{\varrho-1}'$ von b_0 und b_1 unabhängige Substitutionen bezeichnen. Keine dieser Substitutionen S' kann sich auf die Einheit, oder allgemeiner auf eine der Substitutionen des Systems G' reduciren; denn wenn S_i' zu G', folglich auch zu G gehörte, so müsste, da auch US_i' eine Substitution von G ist, dasselbe mit U der Fall sein. Wir behaupten aber, dies sei unmöglich. Man hat nämlich gesehen, dass die Substitutionen S_i von G b_0 und b_1 auf die Plätze von irgend zwei Buchstaben und umgekehrt irgend zwei Buchstaben auf die Plätze von b_0 und b_1 bringen können. Wenn nun U dem Systeme G angehörte, so müsste dasselbe mit allen Substitutionen von der Form $S_i U S_i^{-1}$, d. h. mit allen Transpositionen der Fall sein; der Index von G wäre dann der Voraussetzung zuwider gleich 1.

Dies vorausgesetzt, nehmen wir die ϱ Substitutionen des Systems G' und die ϱ vorhergehenden Substitutionen; diese 2ϱ Substitutionen

$$(3). \qquad \begin{cases} 1 \quad , S_1 \quad , S_2 \quad , \ldots , \; S_{\varrho-1} \, , \\ US_0', US_1', US_2', \ldots , \; US_{\varrho-1}' \end{cases}$$

bilden offenbar ein conjugirtes System. In der That gehören die Produkte $S_i S_j$ und $US_i' \times US_j' = S_i' S_j'$ zu G, und da sie von b_0 und von b_1 unabhängig sind, so sind sie in der ersten Reihe der Tabelle (3) enthalten. Ebenso gehört das Produkt $S_i \times US_j'$

$= U \times S_i S_j'$ dem Systeme G an; dasselbe muss sich in der zweiten Reihe der Tabelle (3) vorfinden. Wir schliessen daraus, dass die Substitutionen

$$(4). \quad \begin{cases} 1 \ , \ S_1 \ , \ S_2 \ , \ \ldots , \ S_{\varrho-1} \ , \\ S_0' \ , \ S_1' \ , \ S_2' \ , \ \ldots , \ S_{\varrho-1}' \end{cases}$$

ein auf $n - 2$ Buchstaben bezügliches System von 2ϱ conjugirten Substitutionen bilden; der Index dieses Systems ist, wie wir behauptet hatten, gleich $\frac{\mu}{2}$.

437. Hilfssatz II. — Es seien G ein System conjugirter Substitutionen, welche aus n Buchstaben $a_0, a_1, a_2, \ldots, a_{n-m-1}, b_0, b_1, \ldots, b_{m-1}$ gebildet sind, und G' das aus denjenigen Substitutionen von G zusammengesetzte System, welche keinen der m Buchstaben b versetzen. Der Index von G kann nicht kleiner als der Index μ von G' sein, und wenn man ihn durch $\mu + \lambda$ darstellt, so lässt sich stets ein System G_1 conjugirter Substitutionen von $n - m$ Buchstaben bilden, dessen Index μ_1 gleich λ oder kleiner als λ ist, und dessen Substitutionen sämmtlich in dem Systeme G enthalten sind.

Wir bezeichnen mit ν die Ordnung von G, mit ϱ die Ordnung von G' und setzen

$$G = 1 \ , \ S_1 \ , \ S_2 \ , \ \ldots , \ S_{\varrho-1} \ , \ \ldots , \ S_{\nu-1} \ ,$$
$$G' = 1 \ , \ S_1 \ , \ S_2 \ , \ \ldots , \ S_{\varrho-1} \ .$$

Man erhält alle Substitutionen der $n - m$ Buchstaben a, wenn man die Substitutionen von G' mit Substitutionen

$$1 \ , \ T_1 \ , \ T_2 \ , \ \ldots , \ T_{\mu-1}$$

multiplicirt, die von den Buchstaben b unabhängig sind. Multiplicirt man auch das System G mit diesen Substitutionen T, so entstehen die $\mu\nu$ Produkte

$$(1). \quad \begin{cases} 1 \ , \ S_1 \ , \ S_2 \ , \ \ldots , \ S_{\varrho-1} \ , \ \ldots , \ S_{\nu-1} \ , \\ T_1 \ , \ T_1 S_1 \ , \ T_1 S_2 \ , \ \ldots , \ T_1 S_{\varrho-1} \ , \ \ldots , \ T_1 S_{\nu-1} \ , \\ \ldots\ldots\ldots\ldots\ldots\ldots \ , \\ T_{\mu-1} \ , \ T_{\mu-1} S_1 \ , \ T_{\mu-1} S_2 \ , \ \ldots , \ T_{\mu-1} S_{\varrho-1} \ , \ \ldots , \ T_{\mu-1} S_{\nu-1} \ , \end{cases}$$

und es lässt sich, wie im vorhergehenden Satze, beweisen, dass diese $\mu\nu$ Substitutionen von einander verschieden sind, dass also

der Index von G nicht kleiner als μ ist. Da dieser Index aber gleich $\mu + \lambda$ und λ von Null verschieden ist, so umfasst die Tabelle (1) nicht alle Substitutionen der n Buchstaben. Die fehlenden $\lambda\nu$ Substitutionen erhält man dadurch, dass man das System G mit gewissen Substitutionen

$$T_1', T_2', \ldots, T_\lambda'$$

multiplicirt, welche sämmtlich von den Buchstaben b abhängen; auf diese Weise entsteht die Tabelle

$$(2). \quad \begin{cases} T_1', T_1'S_1, T_1'S_2, \ldots, T_1'S_{\varrho-1}, \ldots, T_1'S_{\nu-1}, \\ T_2', T_2'S_1, T_2'S_2, \ldots, T_2'S_{\varrho-1}, \ldots, T_2'S_{\nu-1}, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ T_\lambda', T_\lambda'S_1, T_\lambda'S_2, \ldots, T_\lambda'S_{\varrho-1}, \ldots, T_\lambda'S_{\nu-1}, \end{cases}$$

welche die Tabelle (1) ergänzt.

Dies vorausgesetzt, behaupten wir, die Substitutionen der Tabelle (1) seien nicht im Stande, in einer beliebig gewählten Permutation die m Buchstaben b auf irgend welche m Plätze zu bringen. Wäre dies nämlich der Fall, so würde jede Substitution der n Buchstaben dadurch vollzogen werden können, dass man zuerst eine Substitution S ausführte, welche die Buchstaben b auf die vorgeschriebenen Plätze brächte; dann würde noch eine Substitution der Buchstaben a zu vollziehen sein, welche gleichbedeutend ist mit einer der Substitutionen des Systems G', auf die eine Substitution T folgt; die Tabelle (1) würde also alle Substitutionen der n Buchstaben umfassen, was der Voraussetzung widerspricht. Daraus geht hervor, dass man in einer Permutation der n gegebenen Buchstaben m Plätze angeben kann, auf welche es unmöglich ist, mittels einer der Substitutionen (1) beziehungsweise die m Buchstaben b zu bringen. Da es aber offenbar $1 . 2 . 3 \ldots (n - m)$ verschiedene Substitutionen giebt, welche diese Wirkung haben können, so müssen dieselben sämmtlich der Tabelle (2) angehören. Wendet man daher die Substitutionen (2) auf die Permutation

$$T_1'^{-1} A$$

an, so werden sich unter den $\lambda\nu$ erhaltenen Permutationen

$$1 . 2 . 3 \ldots (n - m)$$

vorfinden, in welchen jeder der m Buchstaben b denselben Platz einnimmt. Wenn man aber in dieser Weise verfährt, so wendet

man augenscheinlich auf die Permutation A die Substitutionen an, welche sich durch Multiplication des G ähnlichen Systems

$$1\,,\ T_1'S_1T_1'^{-1}\,,\ T_1'S_2T_1'^{-1}\,,\ \ldots\,,\ T_1'S_{\nu-1}T_1'^{-1}$$

mit den Substitutionen

$$1\,,\ T_2'T_1'^{-1}\,,\ T_3'T_1'^{-1}\,,\ \ldots\,,\ T_\lambda'T_1'^{-1}$$

ergeben. Folglich ist das System G selbst von der Beschaffenheit, dass wenn man seine Substitutionen mit λ passend gewählten Substitutionen

$$1\,,\ U_1\,,\ U_2\,,\ \ldots\,,\ U_{\lambda-1}$$

multiplicirt, die erhaltenen Produkte

$$(3).\qquad \begin{cases} 1\,, & S_1\,, & S_2\,, & \ldots\,, & S_{\nu-1}\,, \\ U_1\,, & U_1S_1\,, & U_1S_2\,, & \ldots\,, & U_1S_{\nu-1}\,, \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ U_{\lambda-1}\,, & U_{\lambda-1}S_1\,, & U_{\lambda-1}S_2\,, & \ldots\,, & U_{\lambda-1}S_{\nu-1} \end{cases}$$

die $1\,.\,2\,.\,3\ldots(n-m)$ Substitutionen umfassen, welche gewisse m Buchstaben nicht versetzen. Diese m Buchstaben sollen mit b_0', b_1', ..., b_{m-1}', die $n-m$ übrigen mit a_0', a_1' ..., a_{n-m-1}' bezeichnet werden. Sind

$$G_1 = 1\,,\ S_1'\,,\ S_2'\,,\ \ldots\,,\ S_{\varrho_1-1}'$$

die ϱ_1 Substitutionen von G, welche die m Buchstaben b' nicht versetzen, so erhält man das System aller

$$1\,.\,2\,.\,3\ldots(n-m)$$

Substitutionen der Buchstaben a', wenn man G_1 mit gewissen von den Buchstaben b' unabhängigen Substitutionen multiplicirt, welche offenbar unter den Factoren $1\,,\ U_1\,,\ U_2\,,\ \ldots\,,\ U_{\lambda-1}$ enthalten sind, und die man durch

$$1\,,\ U_1\,,\ U_2\,,\ \ldots\,,\ U_{\mu_1-1}$$

darstellen kann; dann ist

$$\mu_1\varrho_1 = 1\,.\,2\,.\,3\ldots(n-m),$$

und die Zahl μ_1, die gleich λ oder kleiner als λ ist, drückt den Index des Systems G_1 aus, dessen Substitutionen sämmtlich in G enthalten sind.

438. Nach Herleitung dieser Hilfssätze wenden wir uns zum Beweise der Lehrsätze, die wir im Auge haben.

Lehrsatz I. — Wenn n eine ungerade Zahl und der Index eines Systems conjugirter Substitutionen, die aus n Buchstaben gebildet sind, grösser als 2 ist, so ist dieser Index gleich n oder grösser als n; ist derselbe gleich n, so besteht das conjugirte System aus allen Substitutionen, die man aus $n-1$ Buchstaben bilden kann.

Die Wahrheit des Satzes leuchtet unmittelbar ein, wenn $n=3$ ist; denn in diesem Falle muss der Index des Systems, sobald er grösser als 2 ist, gleich 3 oder grösser als 3 sein. Ist der Index gleich 3, so ist die Ordnung des Systems $\frac{1 \cdot 2 \cdot 3}{3}$ oder 2, also eine Primzahl. Dann besteht das System aus den beiden Potenzen einer cyclischen Substitution zweiter Ordnung, d. h. einer Transposition.

Wir sehen somit, dass wir den vorliegenden Satz in seiner vollen Allgemeinheit begründen, wenn wir seine Richtigkeit für $n=n'$ voraussetzen und auf Grund dieser Annahme beweisen, dass derselbe auch noch für $n=n'+2$ besteht. Mit andern Worten, wir dürfen den Satz als gültig ansehen, wenn darin n durch $n-2$ ersetzt wird; dann bezeichnet n eine ungerade Zahl, die wenigstens gleich 5 ist.

Es seien G das gegebene conjugirte System, dessen Index, wie wir voraussetzen, grösser als 2 ist, und G' das aus denjenigen der Substitutionen von G gebildete conjugirte System, welche zwei aus der Reihe der n gegebenen nach Belieben gewählte Buchstaben nicht versetzen. Unserer Annahme nach kann der Index von G' nicht zu gleicher Zeit grösser als 2 und kleiner als $n-2$ sein. Dieser Index ist daher eine der fünf Zahlen

$$1\,,\ 2\,,\ n-2\,,\ n-1\,,\ n\,,$$

oder aber er ist grösser als n, und in diesem Falle muss der Index von G gleichfalls grösser als n sein. Wir wollen die fünf Fälle, zu denen wir so geführt werden, der Reihe nach in Erwägung ziehen.

1°. Der Index von G' ist 1. — Da der Index von G der Voraussetzung nach nicht 1 ist, so ist derselbe (No. 428 u. No. 429, Zusätze) einer der Zahlen n, $\frac{n(n-1)}{2}$, $n(n-1)$

gleich, und wenn er gleich n ist, so besteht das System G aus allen Substitutionen von $n - 1$ Buchstaben.

2⁰. Der Index von G' ist 2. — In diesem Falle ist der Index von G, den wir als von 2 verschieden voraussetzen, eine der Zahlen $2n$, $n(n-1)$, $2n(n-1)$ (No. 428 und No. 429); er ist daher grösser als n.

3⁰. Der Index von G' ist $n - 2$. — In diesem Falle kann der Index von G nach dem Hilfssatz I (No. 436) nicht gleich $n - 2$ sein, da $n - 2$ eine ungerade Zahl ist. Wenn der Index von G gleich $n - 1$ oder gleich n ist, so lässt sich nach dem Hilfssatz II (No. 437) ein System conjugirter Substitutionen von $n - 2$ Buchstaben bilden, dessen Index 1 oder 2 ist, und dessen Substitutionen sämmtlich im G enthalten sind. Man fällt daher wieder auf eine der beiden vorhergehenden Hypothesen, wenn der Index von G nicht grösser als n ist.

4⁰. Der Index von G' ist $n - 1$. — In diesem Falle kann der Index von G nicht gleich $n - 1$ sein; denn sonst könnte man nach dem Hilfssatz I ein System conjugirter Substitutionen von $n - 2$ Buchstaben bilden, dessen Index $\frac{n-1}{2}$ sein würde. Nun ist die Zahl $\frac{n-1}{2}$, wenn $n > 5$ ist, grösser als 2 und kleiner als $n - 2$; ausserdem setzen wir voraus, dass der Index eines auf $n - 2$ Buchstaben bezüglichen conjugirten Systems nicht zu gleicher Zeit grösser als 2 und kleiner als $n - 2$ sein könne; folglich ist die Hypothese, die wir jetzt erörtern, unzulässig, wenn $n > 5$ ist. Sie ist es aber auch noch für $n = 5$; denn in diesem Falle darf der Index von G' nicht gleich $n - 1 = 4$ vorausgesetzt werden, da 4 kein Divisor des Produkts $1 . 2 . 3$ ist.

Wenn also der Index von G nicht grösser als n ist, so muss er gleich n sein; dann kann man aber nach dem Hilfssatz II ein System conjugirter Substitutionen von $n - 2$ Buchstaben bilden, welches 1 zum Index hat, und dessen Substitutionen sämmtlich in G enthalten sind. Man gelangt auf diese Weise wieder zur ersten der oben betrachteten Hypothesen.

5⁰. Der Index von G' ist n. — In diesem Falle ist der Index von G nothwendig grösser als n; denn da n eine ungerade Zahl ist, so kann derselbe nach dem Hilfssatz I nicht gleich n sein.

Wir schliessen daraus, dass der Index von G, sobald er grösser als 2 ist, in keinem Falle kleiner als n sein kann, und dass, wenn derselbe gleich n ist, das System G aus den Substitutionen von $n-1$ Buchstaben besteht.

439. Lehrsatz II. — Wenn n eine gerade Zahl und der Index eines Systes conjugirter Substitutionen, die aus n Buchstaben gebildet sind, grösser als 2 ist, so muss derselbe gleich n oder grösser als n sein; eine Ausnahme bildet der Fall $n=4$. Ist der Index des Systems gleich n, so besteht letzteres, mit alleiniger Ausnahme des Falles, in welchem $n=6$ ist, aus allen Substitutionen, die sich aus $n-1$ Buchstaben bilden lassen.

Es seien G das gegebene conjugirte System und G_0 ein conjugirtes System, welches aus denjenigen der Substitutionen von G besteht, die einen nach Belieben gewählten Buchstaben nicht versetzen. Wir setzen voraus, der Index von G sei grösser als 2. Was den Index des Systems G_0 betrifft, welches sich nur auf $n-1$ Buchstaben bezieht, so kann derselbe, da $n-1$ eine ungerade Zahl ist, nach dem vorhergehenden Satze nicht zu gleicher Zeit grösser als 2 und kleiner als $n-1$ sein. Der Index von G_0 ist daher eine der Zahlen

$$1, 2, n-1, n,$$

oder aber er ist grösser als n, und in diesem Falle ist auch der Index von G grösser als n. Wir wollen diese vier Hypothesen einzeln verfolgen:

1⁰. Der Index von G_0 ist 1. — In diesem Falle ist der Index von G gleich n (No. 428, Zusatz), da man ihn als von 1 verschieden voraussetzt.

2⁰. Der Index von G_0 ist 2. — In diesem Falle ist der Index von G gleich $2n$ (No. 428), da man ihn als von 2 verschieden voraussetzt.

3⁰. Der Index von G_0 ist $n-1$. — Da $n-1$ ungerade ist, so besteht das System G_0 (No. 438) in diesem Falle aus allen Substitutionen von $n-2$ Buchstaben, und sein Index, der grösser als 1 ist, muss (No. 428 und 429) einer der Zahlen n, $\frac{n(n-1)}{2}$, $n(n-1)$ gleich sein; dabei wird

indess $n > 4$*) vorausgesetzt. Ausserdem kann dieser Index nur dann gleich n sein, wenn G alle Substitutionen von $n-1$ Buchstaben umfasst.

4⁰. Der Index von G_0 ist n. — Dann ist der Index von G gleich n oder grösser als n; wir haben daher nur noch den Fall zu untersuchen, in welchem dieser Index gleich n ist.

Vorher bemerken wir, dass der erste Theil unseres Satzes: Wenn die gerade Zahl n grösser als 4 ist, so kann der Index eines auf n Buchstaben bezüglichen Systems conjugirter Substitutionen nicht zu gleicher Zeit grösser als 2 und kleiner als n sein durch die vorstehende Entwicklung bereits bewiesen ist. Im Folgenden wird $n-2 > 4$, also $n > 6$ vorausgesetzt. Wir bezeichnen mit G' das conjugirte System, welches aus denjenigen der Substitutionen von G_0 besteht, die einen der auf G_0 bezüglichen $n-1$ Buchstaben nicht versetzen; dieser Buchstabe kann übrigens nach Belieben gewählt werden. Der Index von G' kann nicht zu gleicher Zeit grösser als 2 und kleiner als $n-2$ sein; ausserdem ist er nicht grösser als n; sein Werth ist daher eine der fünf Zahlen $1, 2, n-2, n-1, n$. Der Fall, in welchem dieser Index eine der Zahlen $n-2$, $n-1$ wäre, lässt sich durch den Hilfssatz II unmittelbar auf den Fall, in welchem er 1 oder 2 wäre, zurückführen. Wir behaupten nun, dieser letzte Fall könne nicht statthaben. Hätte nämlich G' den Index 1 oder 2, so würde (No. 428) der Index von G_0 eine der Zahlen $1, 2, n-1, 2(n-1)$ sein müssen, von denen keine gleich n sein kann. Der Index von G' ist daher gleich n; dann könnte man aber nach dem Hilfssatz I ein System conjugirter Substitutionen von $n-2$ Buchstaben bilden, dessen Index $\frac{n}{2}$ sein würde, was unmöglich ist, da man

$$2 < \frac{n}{2} < n-2$$

hat. Unsere letzte Hypothese ist daher unzulässig, wenn die Zahl n grösser als 6 ist. Sie kann dagegen, wie wir zeigen werden, stattfinden, wenn $n = 6$ ist. Für $n = 4$ ist sie unmög-

*) Wir haben in No. 427 gesehen, dass man aus vier Buchstaben ein conjugirtes System bilden kann, dessen Ordnung gleich 8, dessen Index folglich gleich 3 ist.

lich; denn der Index von G_0 kann nicht gleich 4 sein, da 4 kein Divisor des Produkts 1 . 2 . 3 ist. Der Fall $n = 6$ bildet somit die einzige Ausnahme vom zweiten Theile unseres Lehrsatzes.

Über das conjugirte System mit dem Index 6, welches 120 Substitutionen von 6 Buchstaben umfasst, welches aber nicht aus den 120 Substitutionen von 5 Buchstaben besteht.

440. Wenn ein solches System existirt, so müssen nach dem vorhergehenden Beweise diejenigen seiner Substitutionen, welche irgend zwei Buchstaben nicht versetzen, ein System conjugirter Substitutionen von vier Buchstaben bilden, dessen Index 6, dessen Ordnung folglich $\frac{1 \cdot 2 \cdot 3 \cdot 4}{6}$ oder 4 ist. Dieses System 4ter Ordnung kann ausser der Einheit nur cyclische Substitutionen 4ter Ordnung, aus zwei Cyclen bestehende regelmässige Substitutionen zweiter Ordnung, oder Transpositionen enthalten. Transpositionen können aber aus dem Grunde darin nicht vorkommen, weil das ganze System der Substitutionen der sechs Buchstaben solche nicht enthalten kann, wie wir im Beweise des Hilfssatzes I (No. 436), welcher den vorliegenden Fall mit umfasst, gesehen haben. Wenn das in Rede stehende System 4ter Ordnung nicht aus den vier Potenzen einer cyclischen Substitution 4ter Ordnung besteht, so umfasst es ausser der Einheit die drei regelmässigen Substitutionen, die sich aus den vier Buchstaben bilden lassen. In allen Fällen findet sich also darin eine durch zwei Transpositionen gebildete regelmässige Substitution vor. Da sich aber sechs Buchstaben 15 mal zu je vier combiniren lassen, so muss das conjugirte System G, mit dem wir uns beschäftigen, 15 regelmässige Substitutionen umfassen, deren jede aus zwei Transpositionen besteht. Zwei Substitutionen dieser Art, welche einen Cyclus und einen dritten Buchstaben gemeinschaftlich hätten, kann es nun in G nicht geben; denn das Produkt von zwei solchen Substitutionen ist offenbar eine cyclische Substitution dritter Ordnung. Vertheilt man daher die 15 Transpositionen der 6 Buchstaben in 5 Gruppen von je 3 Transpositionen, und zwar so, dass die 6 Buchstaben in den 3 Transpositionen ein und derselben Gruppe vorkommen, so erhält man die 15 regelmässigen

Substitutionen von G dadurch, dass man je zwei der ein und derselben Gruppe angehörenden Transpositionen in einander multiplicirt. Jede andere regelmässige Substitution derselben Art hat nothwendig einen Cyclus und einen dritten Buchstaben mit einer dieser 15 Substitutionen gemeinschaftlich, und kann folglich in G nicht enthalten sein. So besitzt dieses System die drei regelmässigen Substitutionen nicht, welche aus denselben vier Buchstaben gebildet sind; es enthält mithin eine cyclische Substitution dieser vier Buchstaben.

Es seien

$$a\,,\,b\,,\,c\,,\,d\,,\,e\,,\,f$$

die gegebenen Buchstaben, und es werde vorausgesetzt, das System G enthalte die Potenzen der cyclischen Substitution

$$U = (a\,,\,b\,,\,c\,,\,d).$$

Dasselbe System muss eine cyclische Substitution U_1 besitzen, welche aus den vier Buchstaben $a\,,\,b\,,\,c\,,\,e$ gebildet ist. Wir dürfen voraussetzen, a sei in U_1 auf den ersten Platz gesetzt; dann kann aber c nicht den dritten Platz einnehmen. Wäre dies nämlich der Fall, so würde das Produkt der beiden regelmässigen Substitutionen U^2 und U_1^2, die einen Factor $(a\,,\,c)$ gemeinschaftlich hätten, nur zwei Transpositionen mit einem gemeinschaftlichen Buchstaben b enthalten und sich auf eine cyclische Substitution dritter Ordnung reduciren, die in G nicht vorkommen kann. Daher muss c in U_1 den zweiten oder den vierten Platz, also in U_1^3 den vierten oder den zweiten Platz einnehmen. Wir werden unter U_1 diejenige dieser beiden Substitutionen verstehen, in welcher c den vierten Platz besetzt; es ist somit

$$U_1 = (a\,,\,b\,,\,e\,,\,c),\ \text{oder}\ U_1 = (a\,,\,e\,,\,b\,,\,c).$$

Ebenso enthält das System G zwei cyclische Substitutionen vierter Ordnung, deren jede der Cubus der andern ist, und welche aus den vier Buchstaben $a\,,\,b\,,\,c\,,\,f$ gebildet sind. Es bezeichne U_2 diejenige dieser Substitutionen, in welcher c den zweiten Platz einnimmt; es sei also

$$U_2 = (a\,,\,c\,,\,f\,,\,b)\,,\ \text{oder}\ U_2 = (a\,,\,c\,,\,b\,,\,f).$$

Nimmt man aber den ersten Werth von U_1, so hat man den zweiten Werth von U_2 zu nehmen, und umgekehrt; denn sonst würden U_1^2 und U_2^2 eine Transposition gemeinschaftlich haben,

und ihr Produkt würde sich auf eine cyclische Substitution dritter Ordnung reduciren. Wir werden

$$U_1 = (a, b, e, c) \ , \ U_2 = (a, c, b, f)$$

machen.

Dies vorausgesetzt, wenden wir der Reihe nach die Substitutionen U, U_1, U_2 auf irgend eine Permutation an; es ergiebt sich

$$U_1 U = (a, e, c, d, b),$$
$$U_2 U_1 U = (a, e, b, c, d, f).$$

Man ersieht daraus, dass das System G die drei cyclischen Substitutionen

$$U = (a, b, c, d) \ , \ T = (a, e, c, d, b) \ , \ S = (a, e, b, c, d, f)$$

enthält, deren Ordnungen beziehungsweise 4, 5, 6 sind. Dies System entsteht also dadurch, dass man die Potenzen von U mit denjenigen von T und die gewonnenen Resultate mit den Potenzen von S zur Rechten oder zur Linken, aber immer in derselben Weise multiplicirt. Dies Verfahren liefert $6 \times 5 \times 4$ oder 120 von einander verschiedene Substitutionen; denn es liegt auf der Hand, dass zwei Produkte wie $S^k T^j U^i$, $S^{k'} T^{j'} U^{i'}$ nur dann einander gleich sein können, wenn $k' = k$, $j' = j$, $i' = i$ ist. Es ist aber noch zu beweisen, dass diese 120 Substitutionen wirklich ein conjugirtes System ausmachen.

Erstens sind die conjugirten Systeme, von denen das eine aus den Potenzen von U, das andere aus den Potenzen von T besteht, gegen einander vertauschbar. Man hat in der That

$$U T U^{-1} = T^2, \ U^2 T U^{-2} = T^4, \ U^3 T U^{-3} = T^8,$$

d. h.

$$U^\nu T U^{-\nu} = T^{2^\nu},$$

und wenn man diese Relation auf die μ^{te} Potenz erhebt, so folgt

$$U^\nu T^\mu U^{-\nu} = T^{\mu \cdot 2^\nu}, \text{ also } U^\nu T^\mu = T^{\mu \cdot 2^\nu} U^\nu.$$

Durch Multiplication dieser beiden Systeme entsteht also ein conjugirtes System von 20 auf 5 Buchstaben bezüglichen Substitutionen. Schriebe man a_0, a_1, a_2, a_3, a_4 statt e, c, d, b, a, so würde dieses System mit dem in No. 424 betrachteten zusammenfallen.

Zweitens ist das conjugirte System

$$1 \ , \ P_1 \ , \ P_2 \ , \ \ldots \ , \ P_{19} \ ,$$

das wir soeben erhalten haben, gegen das conjugirte System vertauschbar, welches durch die Potenzen von S gebildet wird. Zunächst lässt sich leicht bewahrheiten, dass man für jeden Werth von n eine ganze Zahl m von der Beschaffenheit ermitteln kann, dass jede der Substitutionen

$$S^m T S^n \ , \ S^m U S^n$$

sich auf eine der Substitutionen P reducire. Die Zahl m wird durch die Bedingung bestimmt, dass diese Substitutionen den Buchstaben f nicht enthalten dürfen, und man erhält

$S^4 TS = T^2 U = UT,$	$S^3 US = T^4 U = UT^2,$
$S^2 TS^2 = T^4,$	$S^4 US^2 = T^3 U^3 = U^3 T,$
$S^5 TS^3 = U^2,$	$S^2 US^3 = T^3 U^2 = U^2 T^2,$
$STS^4 = T^4 U^3 = U^3 T^3,$	$SUS^4 = T^4 U^2 = U^2 T,$
$S^3 TS^5 = T^2 U^2 = U^2 T^3,$	$S^5 US^5 = U^3.$

Man hat daher für jeden Werth von n

$$S^m TS^n = P_i \ , \ S^m US^n = P_i \, ,$$

oder

$$TS^n = S^{-m} P_i \ , \ US^n = S^{-m} P_i \, ,$$

wo m und i passende Werthe haben. Daraus geht hervor, dass jedes Produkt von der Form $P_j S^\nu$ auf die Form $S^\mu P_k$ gebracht werden kann. P_j ist nämlich ein Produkt, welches aus Factoren T und aus Factoren U besteht, und nach dem Vorhergehenden kann man S^ν einen Platz zur Linken hin vorrücken lassen, wenn man zugleich den Exponenten ν ändert. Nachdem man dies Verfahren hinlänglich oft wiederholt hat, wird $P_j S^\nu$ augenscheinlich in einen Ausdruck von der Form $S^\mu P_k$ verwandelt sein. Da somit das System der Substitutionen P und dasjenige der Potenzen von S gegen einander vertauschbar sind, so entsteht durch Multiplication beider ein conjugirtes System, dessen Ordnung $20 \times 6 = 120$, dessen Index also 6 ist.

Man beachte noch, dass das System, dessen Existenz wir jetzt nachgewiesen haben, ebenso viele Substitutionen erster Art, wie Substitutionen zweiter Art enthält. Seine Substitutionen erster Art machen folglich ein conjugirtes System aus, dessen Ordnung 60 und dessen Index 12 ist.

Transitive Systeme conjugirter Substitutionen.

441. Wenn die Substitutionen eines conjugirten Systems es gestatten, einen der Buchstaben der Reihe nach an die Stelle jedes der andern zu setzen, so heisst das System transitiv, im entgegengesetzten Falle intransitiv. Diese Eintheilung der conjugirten Systeme in transitive und intransitive rührt von Cauchy her; sie ist für die Theorie, die wir hier darlegen, von der grössten Bedeutung.

Wenn allgemeiner die Substitutionen eines conjugirten Systems es gestatten, m der gegebenen Buchstaben auf die Plätze von irgendwelchen m anderen zu bringen, so werden wir das System $m$mal transitiv nennen.

Wenn ein System conjugirter Substitutionen $m$mal transitiv ist, so ermöglichen es seine Substitutionen, m beliebige Buchstaben auf die Plätze von irgend welchen m anderen zu bringen. Da nämlich vorausgesetzt wird, das vorgelegte System sei $m$mal transitiv, so giebt es m Buchstaben $a_1, a_2, \ldots, a_m$, welche auf die Plätze von irgend welchen m anderen $b_1, b_2, \ldots, b_m$, die von den ersteren verschieden oder nicht verschieden sind, gebracht werden können. Umgekehrt gestatten es die Substitutionen des Systems, $a_1, a_2, \ldots, a_m$ durch $b_1, b_2, \ldots, b_m$ zu ersetzen, und sie können folglich diesen letzteren Buchstaben die Plätze von m beliebigen Buchstaben anweisen.

Es leuchtet ein, dass das System aller aus n Buchstaben gebildeten Substitutionen $(n-1)$mal transitiv, das System, welches alle aus diesen Buchstaben gebildeten Substitutionen erster Art umfasst, $(n-2)$mal transitiv ist.

Man sieht auch, dass ein System conjugirter Substitutionen, welche aus n Buchstaben gebildet sind, transitiv ist, wenn es eine cyclische Substitution n^{ter} Ordnung enthält; dies ist aber keine nothwendige Bedingung. Allgemein ist ein conjugirtes System, dass sich auf n Buchstaben bezieht, m mal transitiv, wenn es m cyclische Substitutionen besitzt, deren Ordnungen beziehungsweise $n, n-1, \ldots, n-m+1$ sind. So z. B. ist das System mit dem Index 6, mit dem wir uns in No. 440 beschäftigt haben, und welches aus 120 conjugirten Substitutionen von 6 Buchstaben besteht, 3mal transitiv, da es drei cyclische Sub-

stitutionen umfasst, welche beziehungsweise die Ordnungen 6, 5, 4 haben.

442. Lehrsatz I. — Die Ordnung eines $m$mal transitiven Systems conjugirter Substitutionen von n Buchstaben ist ein Vielfaches von $n(n-1) \ldots (n-m+1)$; mit andern Worten, der Index des Systems ist ein Divisor des Produkts

$$1 . 2 . 3 \ldots (n-m).$$

Es seien $A_0, A_1, A_2, \ldots$ die $n(n-1) \ldots (n-m+1)$ Gruppirungen, die man aus den n gegebenen Buchstaben durch Nebeneinanderstellung von je m derselben bilden kann, und

$$S_0, S_1, S_2, \ldots, S_{\varrho-1}$$

diejenigen der Substitutionen des vorgelegten Systems G, welche die Buchstaben der Gruppirung A_i durch die Buchstaben ersetzen, welche in A_j beziehungsweise dieselben Plätze einnehmen. Bezeichnen wir ausserdem mit T eine der Substitutionen von G, welche die Buchstaben von A_j durch diejenigen von A_k ersetzen, so ist es klar, dass die ϱ Substitutionen

$$TS_0, TS_1, TS_2, \ldots, TS_{\varrho-1}$$

die Buchstaben von A_i durch diejenigen von A_k ersetzen werden. Die Anzahl der Substitutionen, welche A_i durch A_k ersetzen, kann daher nicht kleiner sein, als die Anzahl derjenigen, welche A_i durch A_j ersetzen, und die letztere Zahl kann umgekehrt auch nicht kleiner sein als die erstere.

Daraus geht hervor, dass es in dem vorgelegten Systeme ein und dieselbe Anzahl ϱ von Substitutionen giebt, welche die gegebene Gruppirung A_i durch jede der Gruppirungen $A_0, A_1, A_2, \ldots$ ersetzen. Bezeichnet also μ die Ordnung des Systems G, so ist

$$\mu = n(n-1) \ldots (n-m+1) \times \varrho,$$

und man erhält für den Index von G den Werth

$$\frac{N}{\mu} = \frac{1 . 2 . 3 \ldots n}{\mu} = \frac{1 . 2 . 3 \ldots (n-m)}{\varrho}.$$

Dieser Index ist folglich ein Divisor des Produkts $1 . 2 . 3 \ldots (n-m)$; man sieht auch noch, dass derselbe gleich dem Index des conjugirten Systems ist, welches aus den ϱ Substitutionen besteht, die eine der Gruppirungen A_i durch sich selbst ersetzen. Es ergiebt sich somit der folgende Satz:

Zusatz. — Wenn ein System G conjugirter Substitutionen $m$mal transitiv ist, so bilden diejenigen seiner Substitutionen, welche m willkürlich gewählte Buchstaben unverrückt stehen lassen, ein conjugirtes System G', dessen Index gleich dem Index von G ist.

443. Lehrsatz II. — Ein System conjugirter Substitutionen, dessen Index grösser als 2 ist, kann nicht $m$mal transitiv sein, wenn es eine Substitution enthält, die nicht mehr als m Buchstaben versetzt.

Wir nehmen an, die Zahl i sei gleich m oder kleiner als m, und das vorgelegte System G enthalte eine Substitution S, welche nur i Buchstaben versetzt. Da m wenigstens gleich i ist, und da das System G $m$mal transitiv sein soll, so muss dasselbe eine Substitution T besitzen, welche die in S enthaltenen i Buchstaben durch i willkürlich gewählte Buchstaben ersetzt; folglich enthält G auch die Substitution TST^{-1}, welche irgend eine S ähnliche Substitution ist.

Zerlegen wir die Substitution S in Cyclen:

$$S = C C_1 C_2 \ldots$$

und bilden die ähnliche Substitution

$$S' = C' C_1^{-1} C_2^{-1} \ldots,$$

so gehört das Produkt

$$S' S = C' C$$

dem Systeme G an. Wenn die Ordnung μ des Cyclus C grösser als 2 ist, und man

$$C = (a_0, a_1, a_2, \ldots, a_{\mu-2}, a_{\mu-1})$$

hat, so machen wir

$$C' = (a_0, a_{\mu-1} . a_{\mu-2}, \ldots, a_0, a_1, a_2)$$

und erhalten

$$S S' = (a_0, a_2, a_1).$$

Der Fall $\mu = 3$ ist im Vorhergehenden einbegriffen; es ist dann $C' = C$. Wenn aber $\mu = 2$ ist und man

$$C = (a_0, a_1)$$

hat, so machen wir, da es wenigstens einen in S nicht enthaltenen Buchstaben a_2 giebt,

$$C' = (a_1, a_2),$$

und erhalten auch jetzt noch

$$SS' = (a_0, a_2, a_1).$$

In allen Fällen enthält danach G eine cyclische Substitution dritter Ordnung; wenn also m gleich 3 oder grösser als 3 ist, so gehören alle cyclischen Substitutionen dritter Ordnung dem Systeme G an, dessen Index folglich gleich 1 oder gleich 2 ist. (No. 418).

Diese Untersuchung lässt den Fall $m = 2$ unberücksichtigt; in diesem Falle enthält aber G der Voraussetzung nach eine der aus den gegebenen Buchstaben gebildeten Transpositionen; folglich umfasst es dieselben sämmtlich, und sein Index ist gleich 1.

Zusatz. — Ein 2mal transitives System conjugirter Substitutionen, dessen Index grösser als 2 ist, enthält keine Transposition; ebenso kann ein dreimal transitives System, dessen Index grösser als 2 ist, keine Transposition und keine cyclische Substitution von drei Buchstaben enthalten.

444. Lehrsatz III. — Wenn der Index eines $m$mal transitiven Systems conjugirter Substitutionen, die aus n Buchstaben gebildet sind, grösser als 2 ist, so ist derselbe ein Vielfaches des Produkts $1.2.3 \ldots m$.

Wir wählen nach Belieben m der gegebenen Buchstaben und bilden die

$$M = 1.2.3 \ldots m$$

Permutationen derselben, die wir durch

$$A_0, A_1, A_2, \ldots, A_{M-1}$$

darstellen; die M Substitutionen ebenderselben Buchstaben seien

$$1, T_1, T_2, \ldots, T_{M-1}.$$

Ferner seien

$$1, S_1, S_2, \ldots, S_{\varrho-1}$$

diejenigen Substitutionen des vorgelegten Systems G, welche die eben ausgewählten m Buchstaben unverrückt stehen lassen, welche folglich die Gruppirung A_0 durch A_0 selbst ersetzen. Wie wir im Beweise des Lehrsatzes I (No. 442) gesehen haben, giebt es im Systeme G ϱ Substitutionen, welche im Stande sind, die m Buchstaben von A_0 durch die Buchstaben zu ersetzen, die in A_i

dieselben Plätze einnehmen. Zur Ausführung einer solchen Substitution genügt es offenbar, zuerst eine Substitution des Systems T zu vollziehen, welche die m Buchstaben von A_i auf die vorgeschriebenen Plätze bringt; dann ist nur noch eine Substitution S' von $n-m$ Buchstaben vorzunehmen. Ueberdiess sind die beiden Substitutionen, die wir in Anwendung bringen, gegeneinander vertauschbar, da sie keinen Buchstaben gemeinschaftlich haben, und die ϱM verschiedenen Substitutionen des Systems G, welche eine der Gruppirungen A durch eine andere, aus denselben Buchstaben gebildete ersetzen können, lassen sich durch

$$\begin{array}{lllll}
1 & , S_1 & , S_2 & , \ldots , & S_{\varrho-1} , \\
T_1\, S_0^{(1)} & , T_1\, S_1^{(1)} & , T_1\, S_2^{(1)} & , \ldots , & T_1\, S_{\varrho-1}^{(1)} , \\
T_2\, S_0^{(2)} & , T_2\, S_1^{(2)} & , T_2\, S_2^{(2)} & , \ldots , & T_2\, S_{\varrho-1}^{(2)} , \\
\cdot & \cdot & \cdot & \cdot & \cdot \\
T_{M-1}\, S_0^{(M-1)} & , T_{M-1}\, S_1^{(M-1)} & , \ldots , & & T_{M-1} S_{\varrho-1}^{(M-1)}
\end{array}$$

darstellen, wo $S_i^{(j)}$ ganz allgemein Substitutionen bezeichnet, welche von den in den Gruppirungen A enthaltenen m Buchstaben nicht abhängen. Das Produkt irgend zweier dieser Substitutionen gehört dem Systeme G an; es ist ausserdem von der Form $T_i\, S'$, wo S' eine von den in A enthaltenen m Buchstaben unabhängige Substitution bedeutet; dies Produkt muss sich daher in der vorstehenden Tabelle vorfinden. Daraus geht hervor, dass die $M\varrho$ Substitutionen dieser Tabelle ein conjugirtes System bilden. Zugleich sieht man, dass die Substitutionen S, welche in zwei Substitutionen dieses Systems als Factoren auftreten, nicht einander gleich sein können. Wenn nämlich $j=i$ ist, so kann man offenbar in unserer Tabelle nicht die beiden Substitutionen $T_j\, S$ und $T_i\, S$ finden, und dasselbe ist der Fall, wenn j von i verschieden ist; denn sonst würde man auch $(T_j\, S)\,(T_i\, S)^{-1}$ oder $T_j\, T_i^{-1}$ darin antreffen, was aus dem Grunde unmöglich ist, weil (Lehrsatz II, No. 443) diese Substitution höchstens m Buchstaben versetzt. Die $M\varrho$ Factoren S der vorhergehenden Tabelle, nämlich:

$$\begin{array}{lllll}
1 & , S_1 & , S_2 & , \ldots , & S_{\varrho-1} , \\
S_0^{(1)} & , S_1^{(1)} & , S_2^{(1)} & , \ldots , & S_{\varrho-1}^{(1)} , \\
S_0^{(2)} & , S_1^{(2)} & , S_2^{(2)} & , \ldots , & S_{\varrho-1}^{(2)} , \\
\cdot & \cdot & \cdot & \cdot & \cdot \\
S_0^{(M-1)} , & S_1^{(M-1)} , & S_2^{(M-1)} , & \ldots , & S_{\varrho-1}^{(M-1)}
\end{array}$$

bilden folglich ein System von $M\varrho$ conjugirten Substitutionen, die aus $n - m$ Buchstaben gebildet sind. Die Ordnung $M\varrho$ dieses Systems ist also ein Divisor des Produkts $1 . 2 \cdot 3 \ldots (n-m)$, und man hat

$$\frac{1 . 2 . 3 \ldots (n-m)}{\varrho} = k\,(1 . 2 \ldots m).$$

Das erste Glied dieser Relation ist nun nach dem Lehrsatz I (No. 442) der Index des Systems G; dieser Index ist somit ein Vielfaches von $1 . 2 \ldots m$.

Anmerkung. — Der im Vorstehenden hergeleitete Satz umfasst den Hilfssatz der No. 436 als einen speciellen Fall. Aus unserer Betrachtung geht nämlich folgender Zusatz hervor:

Zusatz. — Wenn ein $m$mal transitives System conjugirter Substitutionen, die aus n Buchstaben gebildet sind, den Index $\mu > 2$ hat, so kann man ein System conjugirter Substitutionen von $n - m$ Buchstaben bilden, dessen Index $\frac{\mu}{1 . 2 \ldots m}$ ist.

445. Lehrsatz IV. — Ein System conjugirter Substitutionen von n Buchstaben, dessen Index grösser als 2 ist, kann nicht mehr als $\frac{n}{2}$ mal transitiv sein*).

Wenn nämlich der Index μ eines $m$mal transitiven Systems conjugirter Substitutionen, die aus n Buchstaben gebildet sind, grösser als 2 ist, so ist dieser Index ein Vielfaches von $1 . 2 . 3 \ldots m$ und zugleich ein Divisor von $1 . 2 . 3 \ldots (n-m)$. Man kann daher nicht

$$m > n - m \text{ oder } m > \frac{n}{2}$$

haben.

Wir können sogar Folgendes hinzufügen:

Wenn n grösser als 6 ist, so giebt es kein auf n Buchstaben bezügliches System conjugirter Substitutionen, dessen Index grösser als 2 und welches $\frac{n}{2}$ mal transitiv ist.

---

*) Die Lehrsätze II und IV sind von Émile Mathieu im Journal de Mathématiques pures et appliquées T. V (2. série) bewiesen.

Wir nehmen an, es gäbe ein System G dieser Art, und eine seiner Substitutionen, T, ersetze die $\frac{n}{2}$ Buchstaben

$$a_0, a_1, a_2, \ldots, a_{\frac{n}{2}-2}, a_{\frac{n}{2}-1}$$

durch

$$a_0', a_1', a_2', \ldots, a'_{\frac{n}{2}-2}, a'_{\frac{n}{2}-1}.$$

Das System G enthält eine Substitution U, welche diese letzteren $\frac{n}{2}$ Buchstaben durch

$$a_0, a_1, a_2, \ldots, a_{\frac{n}{2}-2}, b$$

ersetzt; darin bedeutet b einen von den $\frac{n}{2}$ Buchstaben a, aus welchen die erste Gruppirung besteht, verschiedenen Buchstaben. Die Substitution $UT = S$ reducirt sich nicht auf die Einheit und lässt die Buchstaben

$$a_0, a_1, \ldots, a_{\frac{n}{2}-2}$$

unverrückt stehen; das System G enthält daher eine Substitution, welche nur $\frac{n}{2} + 1$ Buchstaben versetzt.

Wir zerlegen diese Substitution S in Cyclen:

$$S = C C_1 C_2 \ldots;$$

bezeichnet T irgend eine Substitution von G, so ist $TST^{-1} = S'$ eine S ähnliche Substitution von G; wir setzen

$$S' = C' C_1' C_2' \ldots.$$

Da S und S' nur $\frac{n}{2} + 1$ Buchstaben enthalten, so kann man T dergestalt wählen, dass

$$C_1' = C_1^{-1}, \quad C_2' = C_2^{-1}, \ldots$$

ist; man erhält dann

$$SS' = CC'.$$

Die Substitution SS' gehört dem Systeme G an, und man kann sogar die Buchstaben von C', mit Ausnahme eines einzigen, nach Belieben wählen. Wir nehmen an, es sei

$$C = (a_0, a_1, a_2, \ldots, a_{i-1}).$$

Wenn $i = 2$ ist, so reducirt sich C auf (a_0, a_1), und C' wird

von der Form (b_0, b_1) sein, wenn man einen der Buchstaben b_0, b_1 aus der Reihe der in S nicht vorkommenden Buchstaben wählt. Da die Substitution SS' höchstens vier Buchstaben versetzt, so hat man nothwendiger Weise (No. 443)

$$\frac{n}{2} \overline{\overline{<}} 3 \text{ oder } n \overline{\overline{<}} 6.$$

Wenn $i > 2$ ist, so kann man

$$C' = (a_0, b, a_{i-1}, a_{i-2}, \ldots, a_2)$$

machen. Die Wahl des Buchstaben b ist nicht unserer Willkür überlassen; wenn b von a_1 verschieden ist, so ist das Produkt SS' oder CC' gleich (a_0, b) (a_1, a_2), und es ergiebt sich, wie früher, dass n höchstens gleich 6 ist. Ist $b = a_1$, so hat man

$$SS' = (a_0, a_2, a_1),$$

was nur im Falle $n = 4$ statthaben kann, wo der Index des 2mal transitiven Systems 2 ist.

Ueber die Ausdrücke, welche den Index eines intransitiven Systems darstellen können.

446. Es seien G ein intransitives System conjugirter Substitutionen von n Buchstaben, und

$$a_1, a_2, \ldots, a_\alpha$$

die α Buchstaben, welche a_1 vermittels der Substitutionen von G ersetzen kann. Bezeichnen a_i und a_j irgend zwei dieser Buchstaben, so giebt es in G zwei Substitutionen, wie

$$\begin{pmatrix} a_i \ldots \\ a_1 \ldots \end{pmatrix}, \begin{pmatrix} a_j \ldots \\ a_1 \ldots \end{pmatrix}.$$

Nun hat das Produkt aus der Umkehrung der ersten in die zweite Substitution die Wirkung, den Buchstaben a_j durch a_i zu ersetzen; folglich können die Substitutionen von G irgend einen der Buchstaben a auf den Platz irgend eines andern Buchstaben derselben Gruppe bringen. Umgekehrt gehört jeder Buchstabe, welcher in Folge der Substitutionen von G einen Buchstaben a_j ersetzen kann, derselben Gruppe an. Denn wenn eine Substitution von G den Buchstaben a_j durch a ersetzen kann, so wird dieselbe in Verbindung mit einer der vorhergehenden Substitutionen es gestatten, a durch a_1 zu ersetzen, und folglich ist a ein Term der betrachteten Gruppe.

Es sei jetzt b_1 einer der gegebenen Buchstaben, welcher nicht in der vorhergehenden Gruppe enthalten ist. Das soeben dargelegte Schlussverfahren beweist, dass b_1 einer zweiten Gruppe von Buchstaben

$$b_1\ ,\ b_2\ ,\ \ldots\ ,\ b_\beta$$

angehört, welche durch die Substitutionen von G nur gegeneinander vertauscht werden können. So fortfahrend erkennt man, dass die n gegebenen Buchstaben in verschiedene Gruppen

$$\begin{array}{l} a_1\ ,\ a_2\ ,\ \ldots\ ,\ a_\alpha, \\ b_1\ ,\ b_2\ ,\ \ldots\ ,\ b_\beta, \\ c_1\ ,\ c_2\ ,\ \ldots\ ,\ c_\gamma, \\ \ldots\ldots\ldots\ldots, \end{array}$$

in der Weise vertheilt werden können, dass die Substitutionen von G nur die Wirkung haben können, die Buchstaben jeder Gruppe gegeneinander zu vertauschen. Mit anderen Worten, jede Substitution S von G ist von der Form

$$S = A\,.\,B\,.\,C\ldots,$$

wo $A\ ,\ B\ ,\ C\ ,\ \ldots$ Substitutionen sind, welche beziehungsweise nur Buchstaben a, Buchstaben b, Buchstaben c, u. s. w. versetzen.

Es liegt auf der Hand, dass die Substitutionen A ein auf α Buchstaben bezügliches transitives System bilden; ebenso bilden die Substitutionen $B\ ,\ C\ ,\ldots$ transitive Systeme, die sich auf β Buchstaben, auf γ Buchstaben, u. s. w. beziehen. Wir bezeichnen den Index des conjugirten Systems der Substitutionen A mit $\mathfrak{A}$, den Index des Systems G mit $\mathfrak{G}$.

Es kann vorkommen, dass das System der Substitutionen A ebenso viele Substitutionen als G enthält; in diesem Falle hat man

$$\frac{1\,.\,2\,.\,3\ldots n}{\mathfrak{G}} = \frac{1\,.\,2\,.\,3\ldots\alpha}{\mathfrak{A}},$$

folglich

$$(1).\qquad \mathfrak{G} = \frac{1\,.\,2\,.\,3\ldots n}{1\,.\,2\,.\,3\ldots\alpha}\,\mathfrak{A}.$$

Wenn dagegen die Ordnung μ des Systems A kleiner als die Ordnung ν von G ist, so muss es in diesem letzteren Systeme Substitutionen, wie $AT\ ,\ AT'$ geben, welche aus ein und derselben Substitution A und aus zwei von den Buchstaben a unab-

hängigen Substitutionen T, T' zusammengesetzt sind. Da das Produkt einer dieser Substitutionen in die Umkehrung der andern die Buchstaben a nicht versetzt, so enthält G eine gewisse Anzahl ϱ von Substitutionen

$$1\,,\ T_1\,,\ T_2\,,\ \ldots\,,\ T_{\varrho-1}\,,$$

welche von den Buchstaben a nicht abhängen und ein conjugirtes System bilden, das wir mit G' bezeichnen. Ist jetzt $A_1\,T'$ eine der Substitutionen von G, welche den Factor A_1 enthalten, so besitzt dieses System die ϱ Substitutionen

$$A_1\,T'\,,\ A_1\,T'\,T_1\,,\ A_1\,T'\,T_2\,,\ \ldots\,,\ A_1\,T'\,T_{\varrho-1}\,,$$

aber keine andere Substitution mit dem Factor A_1; denn eine solche Substitution kann auf die Form $A_1\,T'\Theta$ gebracht werden, und wenn sie G angehörte, so müsste auch Θ eine Substitution dieses Systems sein.

Da A_1 irgend eine der von Eins verschiedenen $\mu-1$ Substitutionen des Systems A bezeichnet, so sieht man, dass G aus $\mu\varrho$ Substitutionen besteht; man hat also $\nu=\mu\varrho$, oder, wenn $\mathfrak{G}'$ den Index des Systems G' bezeichnet,

$$\frac{1\,.\,2\,.\,3\ldots n}{\mathfrak{G}}=\frac{1\,.\,2\,.\,3\ldots\alpha}{\mathfrak{A}}\times\frac{1\,.\,2\,.\,3\ldots(n-\alpha)}{\mathfrak{G}'}\,,$$

woraus sich

$$(2).\qquad \mathfrak{G}=\frac{1\,.\,2\,.\,3\ldots n}{(1\,.\,2\ldots\alpha)\,[1\,.\,2\ldots(n-\alpha)]}\,\mathfrak{A}\,\mathfrak{G}'$$

ergiebt.

Nimmt man an, dass das System G' sich auf die einzige der Einheit gleiche Substitution reducirt, so hat man

$$\mathfrak{G}'=1\,.\,2\,.\,3\ldots(n-\alpha)\,;$$

daher kann man die Formel (1) als in der Formel (2) enthalten ansehen.

An das System G' lassen sich dieselben Bemerkungen wie an das System G knüpfen, und man erhält folglich

$$\mathfrak{G}'=\frac{1\,.\,2\,.\,3\ldots(n-\alpha)}{(1\,.\,2\,.\,3\ldots\beta)\,[1\,.\,2\ldots(n-\alpha-\beta)]}\,\mathfrak{B}\,\mathfrak{G}''\,,$$

wo $\mathfrak{B}$ der Index eines auf β Buchstaben bezüglichen transitiven Systems und $\mathfrak{G}''$ der Index eines auf $n-\alpha-\beta$ Buchstaben bezüglichen Systems ist.

In dieser Weise kann man fortfahren, bis man in der Reihe G, G', G'', ... ein conjugirtes System antrifft, welches nicht

mehr intransitiv ist; dieses System bezieht sich dann auf die letzte Gruppe der gegebenen Buchstaben. Die vorhergehenden Formeln liefern

$$(3). \qquad \mathfrak{G} = \mathfrak{N}\mathfrak{A}\mathfrak{B}\mathfrak{C}\ldots,$$

wenn

$$\mathfrak{N} = \frac{1.2.3\ldots n}{(1.2.3\ldots\alpha)(1.2.3\ldots\beta)(1.2.3\ldots\gamma)\ldots}$$

gesetzt wird; zugleich ist

$$n = \alpha + \beta + \gamma + \ldots.$$

Die von Cauchy angegebene Formel (3) lehrt uns den Ausdruck der Zahlen kennen, welche geeignet sind, die Indices der intransitiven Systeme darzustellen.

447. Es ist zu beachten, dass die Formel (2) auch in folgender Weise geschrieben werden kann:

$$\mathfrak{G} = \frac{n(n-1)\ldots(n-\alpha+1)}{1.2\ldots\alpha}\mathfrak{A}\mathfrak{G}',$$

und da α nur die Werthe $1, 2, \ldots, (n-1)$ haben kann, so ist der erste Factor dieses Ausdrucks von $\mathfrak{G}$ eine der Zahlen

$$\frac{n}{1}, \frac{n(n-1)}{1.2}, \ldots,$$

von denen n die kleinste ist. Ausserdem sind $\mathfrak{A}$ und $\mathfrak{G}'$ ganze Zahlen, folglich ist $\mathfrak{G}$ wenigstens gleich n. Man sieht sogar, dass, wenn $\mathfrak{G} = n$ sein soll, die Bedingungen

$$\alpha = 1 \text{ oder } = n-1, \mathfrak{A} = 1, \mathfrak{G}' = 1$$

erfüllt sein müssen, und dann besteht das vorgelegte System G offenbar aus den $1.2.3\ldots(n-1)$ Substitutionen von $n-1$ Buchstaben.

Die vorhergehende Formel zeigt noch, dass, wenn $\mathfrak{G}$ grösser als n ist, dieser Index wenigstens gleich dem kleinsten der Werthe $2n, \frac{n(n-1)}{2}$ sein wird.

Obere Grenze der Indices, die grösser als 2 sind, im Falle transitiver Systeme.

448. Wir lassen hier mit einigen Modificationen den Beweis folgen, welchen Cauchy (Comptes rendus de l'Académie des Sciences, T. XXI) für den Satz von Bertrand gegeben hat.

Nach dem Vorhergehenden kann der Index eines intransitiven Systems nicht kleiner als die Anzahl der Buchstaben sein; zur vollständigen Begründung des in Rede stehenden Satzes hat man daher nur noch transitive Systeme in's Auge zu fassen.

Wir behaupten, der Index eines auf n Buchstaben bezüglichen transitiven Systems G könne nicht zu gleicher Zeit grösser als 2 und kleiner als n sein, wofern nicht $n = 4$ ist. Dies zu beweisen, unterscheiden wir drei Fälle:

1°. Das System G ist einmal transitiv. — In diesem Falle ist das System G', welches diejenigen der Substitutionen von G umfasst, die nur $n-1$ Buchstaben versetzen, intransitiv, und sein Index ist gleich $n-1$ oder grösser als $n-1$. Dieser Index stimmt mit dem Index von G überein, und wir behaupten, derselbe könne nicht gleich $n-1$ sein, wenn $n > 4$ ist. Hätte nämlich jedes der beiden Systeme G und G' den Index $n-1$, so würde (No. 447) G' aus den Substitutionen von $n-2$ Buchstaben bestehen, und diese Substitutionen würden dem Systeme G angehören. Nun kann G nicht alle Substitutionen von $n-1$ Buchstaben enthalten; denn sonst wäre es nicht transitiv, oder es wäre aus allen Substitutionen von n Buchstaben zusammengesetzt, in welchem Falle es den Index 1 hätte. Dies vorausgesetzt, kann das System G mit dem Index $n-1$, sobald $n > 4$ ist, nicht alle Substitutionen von $n-2$ Buchstaben umfassen; denn wenn dies der Fall wäre, so würde sein Index nicht $n-1$, sondern (No. 429, Zusatz) eine der Zahlen $\frac{n(n-1)}{2}$, $n(n-1)$ sein. Wenn also $n > 4$ ist, so ist (No. 447) der Index von G oder von G' wenigstens gleich der kleinsten der beiden Zahlen $2(n-1)$, $\frac{(n-1)(n-2)}{2}$. Er ist folglich grösser als n.

2°. Das System G ist zweimal transitiv. — Dann ist das System G' einmal transitiv, und wenn man $n-1 > 4$ hat, so ist der Index dieses Systems, welcher mit dem Index von G übereinstimmt, wenigstens gleich der kleinsten der beiden Zahlen

$$2(n-2) = n + (n-4),$$

$$\frac{(n-2)(n-3)}{2} = n + \frac{(n-1)(n-6)}{2},$$

welche beide nicht kleiner als n sind, sobald $n > 5$ ist. Hinsichtlich des Falles $n = 5$ beziehen wir uns auf den Lehrsatz der No. 433.

3⁰. Das System G ist wenigstens dreimal transitiv. Es seien $a_0, a_1, \ldots, a_{n-1}$ die gegebenen Buchstaben und

$$1, S_1, S_2, \ldots, S_{\mu-1}$$

die Substitutionen von G. Ferner bezeichne T_i die Transposition (a_0, a_i). Multiplicirt man die Substitutionen von G, etwa zur Rechten, mit

$$T_0, T_1, \ldots, T_{n-1},$$

so erhält man $n\mu$ Produkte, die von einander verschieden sind, wenn der Index von G grösser als 2 ist; denn hätte man

$$T_i S_k = T_j S_h,$$

so würde

$$T_i^{-1} T_j = S_k S_h^{-1}$$

sein, und folglich die Substitution $T_i^{-1} T_j$ dem Systeme G angehören. Nun ist dieses Produkt eine cyclische Substitution von drei Buchstaben, wofern nicht einer seiner Factoren gleich 1 ist, in welchem Falle es sich auf eine Transposition reducirt. Nach dem Zusatz der No. 443 kann aber G unter der gemachten Voraussetzung eine solche Substitution nicht besitzen; folglich sind die $n\mu$ erhaltenen Produkte von einander verschieden. Dies erfordert, dass $n\mu$ nicht grösser als $1.2\ldots n$, d. h. dass der Index von G wenigstens gleich n ist.

Viertes Kapitel.

Ueber einige besondere Fälle der Theorie der Substitutionen.

Ueber die linearen Functionen von der Form

$$\frac{ax+b}{a'x+b'}.$$

449. Die nachstehenden Entwicklungen werden uns zu Ergebnissen führen, die vom Standpunkte der Theorie der Substitutionen aus höchst interessant sind; auch werden sie uns späterhin in der Theorie der Gleichungen von Nutzen sein.

Es werde

$$(1). \qquad \vartheta x = \frac{ax+b}{a'x+b'},$$

gesetzt, wo a, b, a', b' irgendwelche gegebene Grössen sind; wir machen ausserdem

$$\vartheta^2 x = \vartheta\vartheta x, \; \vartheta^3 x = \vartheta\vartheta^2 x, \; \ldots, \; \vartheta^m x = \vartheta\vartheta^{m-1} x.$$

Es ist leicht, den allgemeinen Ausdruck von $\vartheta^m x$ zu erhalten. Ist nämlich

$$(2). \qquad \vartheta^m x = \frac{a_m x + b_m}{a'_m x + b'_m},$$

so ergiebt sich aus dem Bildungsgesetze der Functionen $\vartheta^2 x, \vartheta^3 x, \ldots$ sofort

$$(3). \qquad \begin{cases} a_m = a\,a_{m-1} + b\,a'_{m-1}, \\ a'_m = a'a_{m-1} + b'a'_{m-1}, \\ b_m = a\,b_{m-1} + b\,b'_{m-1}, \\ b'_m = a'b_{m-1} + b'b'_{m-1}. \end{cases}$$

Um mittels dieser Gleichungen die Werthe von a_m, a'_m, b_m, b'_m als Functionen der bekannten Grössen a, a', b, b' darzustellen,

bezeichnen wir mit z eine Grösse von der Beschaffenheit, dass

$$\frac{z}{1} = \frac{b + b'z}{a + a'z} \tag{4}$$

ist; dann liefern die Gleichungen (3)

$$a_m + a'_m z = (a + a'z)\,(a_{m-1} + a'_{m-1} z),$$
$$b_m + b'_m z = (a + a'z)\,(b_{m-1} + b'_{m-1} z),$$

und daraus folgt

$$\begin{cases} a_m + a'_m z = (a + a'z)^m, \\ b_m + b'_m z = z(a + a'z)^m. \end{cases} \tag{5}$$

Die Gleichung (4) hat zwei Wurzeln, da sie vom zweiten Grade ist; werden diese Wurzeln mit z und z' bezeichnet, so ist noch

$$\begin{cases} a_m + a'_m z' = (a + a'z')^m, \\ b_m + b'_m z' = z'(a + a'z')^m. \end{cases} \tag{6}$$

Die Gleichungen (5) und (6) bestimmen die Werthe von

$$a_m\,,\; a'_m\,,\; b_m\,,\; b'_m.$$

Setzt man der Kürze wegen

$$2t = \sqrt{(a + b')^2 - 4\,(ab' - ba')}, \tag{7}$$

und

$$\begin{cases} P_m = (a + b' + 2t)^m + (a + b' - 2t)^m, \\ Q_m = \dfrac{(a + b' + 2t)^m - (a + b' - 2t)^m}{2t}, \end{cases} \tag{8}$$

so ergiebt sich leicht

$$\begin{cases} a_m = \dfrac{P_m + (a - b')\,Q_m}{2^{m+1}}, \\ a'_m = a' \dfrac{Q_m}{2^m}, \\ b_m = b \dfrac{Q_m}{2^m}, \\ b'_m = \dfrac{P_m - (a - b')\,Q_m}{2^{m+1}}, \end{cases} \tag{9}$$

aus welchen Gleichungen

$$(10). \quad \begin{cases} \dfrac{a_m - b'_m}{a'_m} = \dfrac{a - b'}{a'}, \\ \dfrac{b_m}{a'_m} = \dfrac{b}{a'}, \\ a_m b'_m - b_m a'_m = (ab' - ba')^m \end{cases}$$

hervorgeht, so dass, wenn

$$ab' - ba' = \pm 1$$

ist, man auch

$$a_m b'_m - b_m a'_m = \pm 1$$

hat.

450. Wir kennen jetzt die Coefficienten von $\vartheta^m x$, ausgedrückt als Functionen der bekannten Grössen a, b, a', b'. Zwar scheint unser Verfahren falsch zu sein, wenn t Null ist; denn in diesem Falle sind die Wurzeln z und z' einander gleich, die Gleichungen (6) also nicht verschieden von den Gleichungen (5). Da aber die Gleichungen (8) und (9) für beliebig kleine Werthe von t stattfinden, so gelten sie auch noch für $t = 0$; man hat in diesem Falle

$$P_m = 2\,(a + b')^m,$$

$$Q_m = 2m\,(a + b')^{m-1},$$

folglich

$$(11). \quad \begin{cases} a_m = \dfrac{(a+b')^m + m\,(a-b')\,(a+b')^{m-1}}{2^m}, \\ a'_m = \dfrac{m a'\,(a+b')^{m-1}}{2^{m-1}}, \\ b_m = \dfrac{m b\,(a+b')^{m-1}}{2^{m-1}}, \\ b'_m = \dfrac{(a+b')^m - m\,(a-b')\,(a+b')^{m-1}}{2^m}. \end{cases}$$

Hier müssen die Grössen a, b, a', b' der Gleichung

$$(12). \qquad (a + b')^2 = 4\,(ab' - ba')$$

genügen, und man kann den Werth von $\vartheta^m x$ in folgender Weise schreiben:

$$\vartheta^m x = \frac{\left(a - b' + \dfrac{a+b'}{m}\right) x + 2b}{2a'x - \left(a - b' - \dfrac{a+b'}{m}\right)}.$$

Lässt man die Zahl m unbegrenzt wachsen, so convergirt $\vartheta^m x$ augenscheinlich gegen die Grösse

$$\frac{(a-b')\,x+2b}{2a'x-(a-b')},$$

welche eine der beiden nach (12) gleichen Constanten

$$\frac{a-b'}{2a'}\,,\quad\frac{-2b'}{a-b'}$$

zum Werth hat.

451. Wir wollen jetzt die Bedingung ermitteln, die erforderlich und hinreichend ist, damit man identisch

$$(13).\qquad \vartheta^\mu x = x\,,$$

das heisst

$$(14).\qquad a_\mu = b'_\mu\,,\ a'_\mu = 0\,,\ b_\mu = 0$$

habe. Man sieht sofort, dass der besondere Fall, in welchem

$$(a+b')^2 = 4\,(ab' - ba')$$

wäre, auszuschliessen ist; denn in diesem Falle könnte, wie die Gleichungen (11) zeigen, den Gleichungen (14) nur dann genügt werden, wenn

$$a+b'=0\,,$$

folglich

$$ab' - ba' = 0$$

wäre; dann würde aber die Function ϑx von x unabhängig sein. Dies vorausgesetzt, ergiebt sich aus den Gleichungen (9), dass die zum Bestehen der Gleichungen (14) erforderliche und hinreichende Bedingung

$$\Omega_\mu = 0,$$

oder

$$(a+b'+2t)^\mu = (a+b'-2t)^\mu$$

ist. Daraus folgt

$$a+b'+2t = (a+b'-2t)\left(\cos\frac{2\lambda\pi}{\mu}+\sqrt{-1}\,\sin\frac{2\lambda\pi}{\mu}\right)$$

und

$$(15).\qquad 2t = (a+b')\,\tan\frac{\lambda\pi}{\mu}\cdot\sqrt{-1}\,;$$

λ bezeichnet eine ganze Zahl, die man als prim zu μ voraussetzen muss, damit die durch ϑ bezeichnete Operation wirklich

μ mal mit x vorzunehmen sei, ehe wieder x zum Vorschein kommt.

Der Vergleich des letzten Werthes von $2t$ mit dem aus (7) hervorgehenden liefert

$$(16). \qquad (a + b')^2 - 4\,(ab' - ba')\cos^2\frac{\lambda\pi}{\mu} = 0,$$

und dies ist die erforderliche und hinreichende Bedingung, damit

$$\vartheta^{\mu} x = x$$

sei.

Setzt man die Grössen a, b, a', b' als reell voraus, so zeigt die Gleichung (16), dass die Grösse $ab' - ba'$ positiv sein muss, ausser wenn $\mu = 2$ ist. Da man nun, ohne die Function ϑx zu ändern, die Constanten a, b, a', b' mit einem beliebigen Factor multipliciren kann, so darf man unbeschadet der Allgemeinheit der Lösung

$$(17). \qquad ab' - ba' = 1$$

voraussetzen; dann liefert die Gleichung (16)

$$(18). \qquad a + b' = 2\cos\frac{\lambda\pi}{\mu}.$$

Wir schreiben vor das zweite Glied nicht das Zeichen $\pm$, da man nöthigenfalls die Zeichen der vier Grössen a, b, a', b' ändern kann. Aus den Gleichungen (17) und (18) folgt

$$(19). \qquad \begin{cases} b' = -\left(a - 2\cos\frac{\lambda\pi}{\mu}\right), \\[2ex] b = -\dfrac{a^2 - 2a\cos\frac{\lambda\pi}{\mu} + 1}{a'}, \end{cases}$$

und die Function ϑx hat den Werth

$$(20). \qquad \vartheta x = \frac{ax - \dfrac{a^2 - 2a\cos\frac{\lambda\pi}{\mu} + 1}{a'}}{a'x - \left(a - 2\cos\frac{\lambda\pi}{\mu}\right)}.$$

Die Grössen a und a' bleiben unbestimmt, und λ bedeutet irgend eine ganze Zahl, die prim zu μ ist. Setzt man immer noch

$$\vartheta^m x = \frac{a_m x + b_m}{a'_m x + b'_m},$$

so erhält man ohne Schwierigkeit

$$(21).\quad \begin{cases} a_m = \dfrac{a \sin \dfrac{m\lambda\pi}{\mu} - \sin \dfrac{(m-1)\lambda\pi}{\mu}}{\sin \dfrac{\lambda\pi}{\mu}}, \\[2ex] a'_m = a' \dfrac{\sin \dfrac{m\lambda\pi}{\mu}}{\sin \dfrac{\lambda\pi}{\mu}}, \\[2ex] b_m = - \dfrac{a^2 - 2a \cos \dfrac{\lambda\pi}{\mu} + 1}{a'} \cdot \dfrac{\sin \dfrac{m\lambda\pi}{\mu}}{\sin \dfrac{\lambda\pi}{\mu}}, \\[2ex] b'_m = \dfrac{\sin \dfrac{(m+1)\lambda\pi}{\mu} - a \sin \dfrac{m\lambda\pi}{\mu}}{\sin \dfrac{\lambda\pi}{\mu}}. \end{cases}$$

Aus den Gleichungen (19) und (21) ergiebt sich

$$(22).\quad \begin{cases} b'_m = -\left(a_m - 2\cos \dfrac{m\lambda\pi}{\mu}\right), \\[2ex] b_m = - \dfrac{a_m^2 - 2a_m \cos \dfrac{m\lambda\pi}{\mu} + 1}{a'_m}, \end{cases}$$

und

$$(23).\quad \begin{cases} a = \dfrac{a_m \sin \dfrac{\lambda\pi}{\mu} + \sin \dfrac{(m-1)\lambda\pi}{\mu}}{\sin \dfrac{m\lambda\pi}{\mu}}, \\[2ex] a' = a'_m \dfrac{\sin \dfrac{\lambda\pi}{\mu}}{\sin \dfrac{m\lambda\pi}{\mu}}, \\[2ex] b = - \dfrac{a_m^2 - 2a_m \cos \dfrac{m\lambda\pi}{\mu} + 1}{a'_m} \cdot \dfrac{\sin \dfrac{\lambda\pi}{\mu}}{\sin \dfrac{m\lambda\pi}{\mu}}, \\[2ex] b' = \dfrac{\sin \dfrac{(m+1)\lambda\pi}{\mu} - a_m \sin \dfrac{\lambda\pi}{\mu}}{\sin \dfrac{m\lambda\pi}{\mu}}. \end{cases}$$

Diese Formeln ermöglichen die Lösung folgender Aufgabe:

Es ist eine lineare Function $\dfrac{a_m x + b_m}{a'_m x + b'_m}$ gegeben; man

soll eine lineare Function $\vartheta x = \frac{ax+b}{a'x+b'}$ ermitteln, die so beschaffen ist, dass man identisch

$$\vartheta^m x = \frac{a_m x + b_m}{a'_m x + b'_m} \quad \text{und} \quad \vartheta^\mu x = x$$

hat.

Die Aufgabe ist offenbar nur dann möglich, wenn die gegebenen Grössen a_m, b_m, a'_m, b'_m den Gleichungen (22) genügen.

Rationale lineare Functionen in Beziehung auf einen Primzahlmodul.

452. Wir wollen hier die rationalen linearen Functionen der Form

$$(1). \qquad \vartheta z = \frac{az+b}{a'z+b'},$$

worin z eine unabhängig Veränderliche ist, von einem besonderen Gesichtspunkte aus betrachten. Die Constanten a, b, a', b' werden als ganze Zahlen vorausgesetzt, die positiv, Null oder negativ sein können. Ausserdem werden wir die Resultate nach einer ungeraden Primzahl p als Modul nehmen, d. h. wir werden die nach dem Modul p congruenten ganzen Zahlen als äquivalent ansehen. Die nachfolgenden Entwicklungen führen zu Resultaten, die nicht nur für die Zahlentheorie äusserst interessant, sondern auch in der Theorie der Substitutionen von grossem Nutzen sind; ich habe dieselben zum ersten Male in den Comptes rendus de l'Académie des Sciences T. XLVIII vorgelegt.

Da wir den Fall, in welchem ϑz sich auf eine Constante reducirt, unberücksichtigt lassen, so wird die Differenz $ab' - ba'$ nach dem Modul p nie congruent Null sein können; diese Differenz soll die Determinante der linearen Function ϑz heissen. Man kann nun, ohne ϑz zu ändern, die Constanten a, b, a', b' mit ein und derselben Zahl k multipliciren; dadurch wird die Determinante mit k^2 multiplicirt; dieselbe ist folglich nach der Multiplication quadratischer Rest oder quadratischer Nichtrest von p, je nachdem sie vor der Multiplication Rest oder Nichtrest war. Danach können die in Rede stehenden linearen Functionen in zwei Klassen eingetheilt werden: Die erste Klasse umfasst diejenigen Functionen, deren Determinante quadratischer Rest von

p ist, während die Functionen, deren Determinante Nichtrest von p ist, die zweite Klasse ausmachen. Es lässt sich aber, wie man sieht, stets so einrichten, dass die Determinante in der ersten Klasse ein beliebig gegebener quadratischer Rest, z. B. 1, ist, und ebenso kann man bewirken, dass die Determinante in der zweiten Klasse ein beliebig gegebener Nichtrest ist.

Der allgemeine Ausdruck von ϑz umfasst ganze und gebrochene Functionen; die ersteren können auf die Form

(2). $$f + \Delta z,$$

die letzteren auf die Form

(3). $$f - \frac{\Delta}{z+g}$$

gebracht werden; Δ bezeichnet in beiden Fällen die Determinante der Function.

Die Determinante Δ kann in den Formeln (2) und (3) die $p-1$ Werthe

$$1\,,\,2\,,\,\ldots\,,\,p-1$$

annehmen, unter denen es ebenso viele Reste wie Nichtreste giebt; die Constanten f und g können dieselben Werthe, und ausserdem noch den Werth Null haben. Daraus folgt, dass die Anzahl der ganzen Functionen, wenn die Veränderliche z selbst mitgezählt wird, $p\,(p-1)$ ist, und dass der Ausdruck (3) $p^2\,(p-1)$ gebrochene Functionen enthält. Die Gesammtzahl N der nach dem Modul p genommenen linearen Functionen ist somit

(4). $$N = (p+1)\,p\,(p-1),$$

und jede der beiden oben unterschiedenen Klassen besteht aus $\frac{1}{2}\,N$ Functionen.

453. Es seien ϑz und $\vartheta_1 z$ zwei nach dem Modul p genommene rationale lineare Functionen. Der Kürze wegen werden wir unter dem Produkt der linearen Function ϑz in $\vartheta_1 z$ das Resultat $\vartheta\vartheta_1 z$ verstehen, welches man erhält, wenn man die Veränderliche z zuerst der mit ϑ_1 bezeichneten Operation unterwirft und mit dem Ergebnisse $\vartheta_1 z$ sodann die Operation vornimmt, welche ϑ andeutet. Diese Definition lässt sich ohne Weiteres auf den Fall von drei, vier, u. s. w. linearen Functionen ausdehnen. Das Produkt von m linearen Functionen, deren jede gleich ϑz ist, d. h. das Resultat, welches man erhält, wenn

man m mal an z die Operation ϑ ausführt, soll die m^{te} Potenz von ϑz heissen und durch $\vartheta^m z$ dargestellt werden.

Die Determinante des Produkts zweier linearen Functionen ist gleich dem Produkte der Determinanten der Factoren. Setzt man nämlich

$$\vartheta z = \frac{a z + b}{a' z + b'} \ , \ \vartheta_1 z = \frac{a_1 z + b_1}{a'_1 z + b'_1} \ ,$$

so ergiebt sich

$$\vartheta \vartheta_1 z = \frac{(a a_1 + b a'_1) z + (a b_1 + b b'_1)}{(a' a_1 + b' a'_1) z + (a' b_1 + b' b'_1)} = \frac{A z + B}{A' z + B'}$$

und

$$(AB' - BA') = (ab' - ba') \ (a_1 b'_1 - b_1 a'_1).$$

Man schliesst daraus, dass das Produkt beliebig vieler linearen Functionen eine lineare Function ist, deren Determinante gleich ist dem Produkte der Determinanten der Factoren. Dies Produkt gehört also der ersten oder der zweiten Klasse an, je nachdem die Anzahl seiner Factoren zweiter Art gerade oder ungerade ist.

Es liegt auf der Hand, dass die Gesammtheit aller linearen Functionen eine Gruppe von der Beschaffenheit bildet, dass das Produkt mehrerer Functionen der Gruppe sich auch in derselben vorfindet. Ebenso ist es nach dem Vorhergehenden mit der Gesammtheit aller linearen Functionen erster Art, nicht aber mit der Gesammtheit der Functionen zweiter Art.

454. Wir betrachten die Reihe

$$(5). \qquad z \ , \ \vartheta z \ , \ \vartheta^2 z \ , \ \vartheta^3 z \ , \ \ldots \ ,$$

welche aus der Veränderlichen z und den nach dem Primzahlmodul p genommenen verschiedenen Potenzen der linearen Function ϑz besteht. Da die Anzahl der linearen Functionen beschränkt ist, so kann die vorstehende Reihe immer nur eine endliche Anzahl nach dem Modul p verschiedener Werthe liefern; folglich müssen einige Terme der Reihe unendlich oft wiederkehren. Angenommen, es sei identisch

$$\vartheta^{n+m} z \equiv \vartheta^m z \text{ oder } \vartheta^n \vartheta^m z \equiv \vartheta^m z \ (mod. \ p) \ ,$$

so werden wir z statt $\vartheta^m z$ schreiben können, und erhalten die Identität

$$(6). \qquad \vartheta^n z \equiv z \ (mod. \ p),$$

woraus leicht für alle ganzen und positiven Werthe von λ und ϱ

$$\vartheta^{\lambda n+\varrho} z \equiv \vartheta^{\varrho} z \ (mod.\ p)$$

folgt. Wir wollen diese Formel auf alle ganzen Werthe von ϱ, dieselben mögen positiv, Null oder negativ sein, ausdehnen, so dass im Besonderen

(7). $$\vartheta^0 z \equiv z \ (mod.\ p),$$

und

(8). $$\vartheta^{-1} z \equiv \vartheta^{n-1} z \ (mod.\ p.)$$

ist.

Bezeichnet n die kleinste Zahl, für welche die Congruenz (6) identisch besteht, so enthält die Reihe (5) nur die n verschiedenen Terme

(9). $$z\,,\ \vartheta z\,,\ \vartheta^2 z\,,\ \ldots\,,\ \vartheta^{n-1} z,$$

und zwei beliebige dieser Terme (9) sind wirklich nach dem Modul p incongruent, wenigstens so lange z unbestimmt bleibt. Die Zahl n soll die Ordnung der linearen Function ϑz für den Modul p heissen.

Bezeichnet e eine Zahl, die prim zu n und kleiner als n ist, so ist die Function $\vartheta^e z$ ebenso wie ϑz von der Ordnung n; denn wenn man die Terme der Reihe (9) an die n Theilpunkte eines in n gleiche Theile getheilten Kreises setzt und darauf vom ersten Terme zum e^{ten}, von da zum $2e^{\text{ten}}$, u. s. w. übergeht, d. h. die Reihe

$$z\,,\ \vartheta^e z\,,\ \vartheta^{2e} z\,,\ \ldots$$

durchläuft, so wird man offenbar alle n Terme antreffen, ehe man in den Ausgangspunkt zurückgelangt. Haben aber die Zahlen n und e den grössten gemeinschaftlichen Divisor $d > 1$, so gelangt man zum Ausgangspunkt zurück, nachdem man $\frac{n}{d}$ Terme angetroffen hat, und die Ordnung der Function $\vartheta^e z$ ist somit gleich $\frac{n}{d}$.

Die Function $\vartheta^{-1} z$, welche durch die Congruenz (8) definirt wird, soll die Umkehrung von ϑz heissen. Ihr Werth lässt sich unmittelbar bestimmen. Ersetzt man nämlich in der Congruenz (1) z durch $\vartheta^{-1} z$, so folgt

$$\vartheta\vartheta^{-1} z = z = \frac{a\vartheta^{-1} z + b}{a'\vartheta^{-1} z + b'},$$

mithin ist

$$(10). \qquad \vartheta^{-1} z = \frac{-b'z + b}{a'z - a}.$$

Dieser Formel zufolge geht die eine der beiden Functionen ϑz und $\vartheta^{-1} z$ aus der andern dadurch hervor, dass man a und b' in $-b'$ und $-a$ verwandelt.

455. Es sei, wie früher,

$$(11). \qquad \vartheta z = \frac{az + b}{a'z + b'},$$

und es werde ausserdem

$$\vartheta^m z = \frac{a_m z + b_m}{a'_m z + b'_m}$$

gesetzt. Macht man der Kürze wegen, wie in No. 449,

$$(12). \qquad 2t = \sqrt{(a + b')^2 - 4(ab' - ba')},$$

$$(13). \qquad \begin{cases} P_m = (a + b' + 2t)^m + (a + b' - 2t)^m, \\[2ex] Q_m = \dfrac{(a + b' + 2t)^m - (a + b' - 2t)^m}{2t}, \end{cases}$$

so erhält man die schon betrachteten Gleichungen

$$(14). \qquad \begin{cases} a_m = \dfrac{P_m + (a - b')Q_m}{2^{m+1}}, \quad b_m = b\,\dfrac{Q_m}{2^m}, \\[2ex] a'_m = a'\,\dfrac{Q_m}{2^m}, \quad b'_m = \dfrac{P_m - (a - b')Q_m}{2^{m+1}}, \end{cases}$$

welche in den Formeln

$$(15). \qquad a_m + b'_m = \frac{P_m}{2^m}, \quad \frac{a_m - b'_m}{a - b'} = \frac{b_m}{b} = \frac{a'_m}{a'} = \frac{Q_m}{2^m}$$

enthalten sind. Bezeichnen wir mit $\varDelta$ die Determinante $ab' - ba'$ der Function ϑz, und mit $\varDelta_m$ die Determinante von $\vartheta^m z$, und setzen ausserdem

$$(16). \qquad 2t_m = \sqrt{(a_m + b'_m)^2 - 4(a_m b'_m - b_m a'_m)},$$

so ergiebt sich aus den Formeln (14) oder (15)

$$(17). \qquad \frac{t_m}{t} = \frac{Q_m}{2^m}, \quad \varDelta_m = \varDelta^m.$$

Geht man daher von ϑz zur m^{ten} Potenz $\vartheta^m z$ dieser Function über, so ist das Verhältniss jeder der Grössen $a - b'$, b, a', t

zu der entsprechenden neuen Grösse dasselbe, und die Determinante wird durch ihre m^{te} Potenz ersetzt. Diese letztere Eigenschaft geht übrigens schon aus den obigen Entwicklungen hervor.

Die Formeln (14) zeigen, dass $\vartheta^m z$ keinen ganzen Werth ausser z annehmen kann, wofern nicht ϑz selbst eine ganze Function ist; denn wenn a' von Null verschieden ist, so kann a'_m nur für $Q_m = 0$ verschwinden, und in diesem Falle hat man $b_m = 0$ und $a_m = b'_m$.

Die nothwendige und hinreichende Bedingung zum Bestehen der Congruenz (6) ist

$$(18). \qquad Q_n \equiv 0 \ (mod.\ p).$$

Damit aber n wirklich die Ordnung der Function ϑz sei, ist ausserdem erforderlich, dass Q_m für jeden Werth m, der kleiner als n ist, von Null verschieden sei. Wir abstrahiren hier von dem Falle, in welchem ϑz von der ersten Ordnung ist, d. h. in welchem sich ϑz auf z reducirt.

Wir wollen jetzt die linearen Functionen ϑz mit Rücksicht auf ihre Ordnung in's Auge fassen. In dieser Untersuchung ist es zweckmässig, drei Fälle zu unterscheiden, je nachdem die Grösse t^2 nach dem Modul p congruent Null, quadratischer Rest oder quadratischer Nichtrest von p ist.

456. Zuerst betrachten wir den Fall, in welchem t^2 nach dem Modul p der Null congruent ist; dann geht die Congruenz (18) über in

$$2n\,(a + b')^{n-1} \equiv 0 \ (mod.\ p).$$

Es kann nun nicht $a + b' \equiv 0 \ (mod.\ p)$ sein, denn sonst würde sich die Bedingung $t \equiv 0 \ (mod.\ p)$ auf

$$ab' - ba' \equiv 0 \ (mod.\ p)$$

reduciren; die Determinante von ϑz wäre also Null, und diese Function selbst eine Constante. Die Congruenz (18) kann daher nur stattfinden, wenn n ein Vielfaches von p ist, und folglich ist die Ordnung der linearen Function ϑz im vorliegenden Falle immer gleich dem Modul p. Die Bedingung $t \equiv 0 \ (mod.\ p)$ liefert

$$a + b' \equiv 2\sqrt{\varDelta} \ (mod.\ p);$$

daraus geht hervor, dass die Determinante Δ quadratischer Rest von p ist; die Function ϑz gehört mithin der ersten Klasse an.

Man erhält alle linearen Functionen p^{ter} Ordnung, wenn man alle verschiedenen Lösungssysteme der beiden Congruenzen

$$a + b' \equiv 2\sqrt{\Delta}\ ,\ ab' - ba' \equiv \Delta\ (mod.\ p)$$

nimmt. Will man zunächst die ganzen Functionen ermitteln, so setze man $a' = 0$, $b' = 1$, so dass $a = \Delta = 1$ ist; man erhält also die $p - 1$ Functionen p^{ter} Ordnung

$$\vartheta z = z + b, \tag{19}$$

wenn man b der Reihe nach die Werthe

$$1, 2, \ldots, p - 1$$

ertheilt. Um die gebrochenen Functionen zu bestimmen, werden wir $a' = 1$ machen und

$$a - b' \equiv 2g$$

setzen, woraus sich

$$a = \sqrt{\Delta} + g, b' = \sqrt{\Delta} - g\ ,\ b = -g^2$$

ergiebt. Der allgemeine Ausdruck der gebrochenen Functionen p^{ter} Ordnung ist somit:

$$\vartheta z = \frac{(\sqrt{\Delta} + g)\ z - g^2}{z + (\sqrt{\Delta} - g)} = g + \sqrt{\Delta} - \frac{\Delta}{z + \sqrt{\Delta} - g}. \tag{20}$$

Die Grösse g kann die p Werthe

$$0, 1, 2, \ldots, p - 1,$$

die Grösse $\sqrt{\Delta}$ dieselben Werthe mit Ausnahme von Null annehmen. Man erhält also $p(p - 1)$ gebrochene Functionen, so dass die Gesammtzahl N_p der linearen Functionen p^{ter} Ordnung folgende ist:

$$N_p = (p + 1)\ (p - 1). \tag{21}$$

Da jede Zahl, die kleiner als p ist, prim zu p sein muss, so haben alle Potenzen einer linearen Function p^{ter} Ordnung gleichfalls die Ordnung p. Daraus folgt, dass die N_p Functionen, deren Existenz wir soeben dargethan haben, $p + 1$ Gruppen bilden, deren jede $p - 1$ Functionen umfasst, welche die Potenzen irgend einer von ihnen sind. Die in Formel (19) enthaltenen $p - 1$ Functionen machen offenbar eine dieser Gruppen aus. Die übrigen p Gruppen liefert die Formel (20), wenn man jeden

der p Werthe von g der Reihe nach mit dem Systeme der $p-1$ Werthe von $\sqrt{\Delta}$ verbindet. Bildet man nämlich die m^{te} Potenz der durch die Gleichung (20) gegebenen Function ϑz, so erhält man bei Anwendung der Formeln (14) oder (15)

$$(22). \qquad \vartheta^m z = \frac{\left(\frac{1}{m}\sqrt{\Delta} + g\right) z - g^2}{z + \left(\frac{1}{m}\sqrt{\Delta} - g\right)},$$

und dieser Ausdruck geht aus dem Ausdruck von ϑz dadurch hervor, dass man $\sqrt{\Delta}$ in $\frac{1}{m}\sqrt{\Delta}$ verwandelt.

457. Wenn die Grösse t^2 von Null verschieden ist, so kann die Congruenz (18), nämlich

$$(23). \qquad (a + b' + 2t)^n \equiv (a + b' - 2t)^n \pmod{p}$$

auf die Form

$$(24). \qquad a + b' + 2t \equiv i\,(a + b' - 2t) \pmod{p}$$

gebracht werden, wo i eine Wurzel der Congruenz

$$(25). \qquad i^n \equiv 1 \pmod{p}$$

bezeichnet. Damit ausserdem n wirklich die Ordnung der Function ϑz sei, muss i eine primitive Wurzel der vorstehenden Congruenz sein.

Setzt man den aus Formel (12) genommenen Werth von t in die Congruenz (24) ein, und schafft das dadurch eingeführte Wurzelzeichen fort, indem man die Congruenz quadrirt, so folgt

$$(26). \qquad \frac{(a+b')^2}{(ab' - ba')} \equiv \frac{(i+1)^2}{i} \pmod{p}.$$

Dies ist die Bedingung, welcher die Constanten a, b, a', b' genügen müssen, wenn die Zahl n, unter der Voraussetzung, dass t von Null verschieden ist, die Ordnung der Function ϑz sein soll. Setzt man

$$(27). \qquad a - b' = 2g,$$

so kann man die Grössen a, b', ba' und die Determinante Δ mittels der Formeln (12), (24) und (27) als Functionen von g, t, i darstellen; es ergiebt sich

$$(28). \quad \begin{cases} a = \dfrac{i+1}{i-1}\, t + g, \\ b' = \dfrac{i+1}{i-1}\, t - g, \\ ba' = t^2 - g^2, \\ \Delta = \dfrac{4 i t^2}{(i-1)^2}. \end{cases}$$

Diese Formeln werden uns zur Construction der linearen Functionen dienen, die wir betrachten; wenn a' von Null verschieden ist, so kann man $a' = 1$ machen. Auch die m^{te} Potenz von ϑz, nämlich

$$\vartheta^m z = \frac{a_m z + b_m}{a'_m z + b'_m}$$

lässt sich leicht bilden; bei Benutzung der Formeln (14) oder (15) erhält man, wenn man noch einen gemeinschaftlichen Factor unterdrückt,

$$(29). \quad a_m + b'_m = 2t\, \frac{i^m + 1}{i^m - 1}, \; a_m - b'_m = a - b', \; a'_m = a', \; b_m = b.$$

Der Uebergang vom Ausdruck von ϑz zu demjenigen von $\vartheta^m z$ erfolgt also einfach dadurch, dass man i durch i^m ersetzt, die Werthe von g und von t jedoch unverändert lässt.

458. Nehmen wir an, die Grösse

$$t^2 = \left(\frac{a+b'}{2}\right)^2 - (ab' - ba')$$

sei quadratischer Rest des Moduls p. Dann ist jede der beiden beziehungsweise durch die Formeln (12) und (24) definirten Grössen t und i reell; folglich kann i nur in dem Falle primitive Wurzel der Congruenz (25) sein, in welchem die Ordnung n der Function ϑz gleich $p-1$ oder gleich einem Divisor von $p-1$ ist. Die linearen Functionen, welche einer primitiven Wurzel i der Congruenz (25) entsprechen, können mittels der Formeln (28) leicht gebildet werden.

Um zunächst die ganzen Functionen zu erhalten, hat man $a' = 0$, $b' = 1$ zu setzen; es ergeben sich die beiden Lösungen

$$t = g = \frac{i-1}{2}, \; a = i \text{ und } t = -g = \frac{i-1}{2i}, \; a = \frac{1}{i},$$

welche die $2p$ ganzen Functionen $iz + b$, $\frac{1}{i} z + b$ liefern, wenn

man b der Reihe nach die Werthe $0, 1, 2, \ldots, p-1$ ertheilt. Wir werden aber nur die p Functionen, welche in der ersten Formel

$$(30). \qquad iz + b$$

enthalten sind, als zur Wurzel i gehörig ansehen; die p übrigen Functionen beziehen sich, wenn $n > 2$ ist, auf die primitive Wurzel $\frac{1}{i}$; in dem besondern Falle $n = 2$ fallen sie mit denen der Formel (30) zusammen.

Um zweitens die gebrochenen Functionen zu erhalten, hat man in den Formeln (28) $a' = 1$ zu machen und findet

$$(31). \quad \begin{cases} a = \frac{i+1}{i-1}\, t + g \;,\; b = t^2 - g^2 \;,\; a' = 1 \\ b' = \frac{i+1}{i-1}\, t - g \;,\; \varDelta = \frac{4\,i\,t^2}{(i-1)^2}\,. \end{cases}$$

Die Verwandlung von t in $-t$ ist für diese Formeln gleichbedeutend mit der Verwandlung von i in $\frac{1}{i}$. Soll man daher der Reihe nach alle Wurzeln i in Anwendung bringen, so kann man sich darauf beschränken, t alle $\frac{p-1}{2}$ Werthe

$$1, 2, \ldots, \frac{p-1}{2}$$

zu ertheilen. Die Grösse g kann die p Werthe

$$0, 1, 2, \ldots, p-1$$

annehmen. Man erhält somit durch die Formeln (31) $\frac{p(p-1)}{2}$ auf die Wurzel i bezügliche gebrochene Functionen, so dass dieser Wurzel im Ganzen $p + \frac{p(p-1)}{2} = \frac{1}{2}(p+1)\,p$ lineare Functionen entsprechen. Dies findet auch noch im Falle $n = 2$ statt, obwohl dann die Congruenz (25) nur die eine primitive Wurzel -1 hat; denn da diese Wurzel ihrer Umkehrung gleich ist, so bleiben die Formeln (31) bei der Verwandlung von t in $-t$ unverändert.

Man erkennt leicht, dass die auf eine primitive Wurzel i bezüglichen $\frac{1}{2}(p+1)\,p$ Functionen von denjenigen verschieden sind, die zu einer andern primitiven Wurzel gehören. Bezeichnet also $\varphi(n)$ die Anzahl der primitiven Wurzeln der Congruenz (25), so giebt es

$$\tfrac{1}{2}(p+1)\,p\varphi(n)$$

Functionen n^{ter} Ordnung, für welche t^2 quadratischer Rest von p ist. Im Besonderen ist die Anzahl der linearen Functionen $(p-1)^{\text{ter}}$ Ordnung gleich

$$\tfrac{1}{2}(p+1)\,p\;\varphi(p-1);$$

hier bezeichnet $\varphi(p-1)$ die Anzahl der primitiven Wurzeln der Primzahl p.

Was die Gesammtzahl der linearen Functionen betrifft, für welche t^2 quadratischer Rest von p, und deren Ordnung n folglich ein Divisor von $p-1$ ist, so ist dieselbe durch die Formel

$$N_{p-1} = \tfrac{1}{2}(p+1)\,p\Sigma\varphi(n)$$

gegeben; der Ausdruck $\Sigma\varphi(n)$, welcher sich über alle Divisoren von $p-1$, mit Ausnahme von 1, erstreckt, ist bekanntlich gleich $p-2$; folglich ist

$$(32).\qquad N_{p-1} = \tfrac{1}{2}(p+1)\,p(p-2).$$

Diese N_{p-1} linearen Functionen können in $\frac{1}{2}(p+1)p$ Gruppen getheilt werden, deren jede $p-2$ Functionen enthält. Es sind dies die $p-2$ Potenzen einer linearen Function $(p-1)^{\text{ter}}$ Ordnung, welche sich auf eine gegebene primitive Wurzel von p bezieht.

Es liegt nämlich auf der Hand, dass die N_{p-1} Functionen, die wir betrachten, sämmtlich durch die Formeln (30) und (31) gegeben werden, wenn man alle Wurzeln der Congruenz

$$i^{p-1} - 1 \equiv 0 \ (mod.\ p),$$

mit Ausnahme von 1, benutzt, und diese Wurezln sind nichts Anderes, als die $p-2$ ersten Potenzen einer primitiven Wurzel i. Wendet man nun diese primitive Wurzel an, so liefern die Gleichungen (30) und (31) $\frac{1}{2}(p+1)p$ Functionen $(p-1)^{\text{ter}}$ Ordnung. Ferner gehen die Potenzen dieser Functionen, wie die Formeln (29) lehren, aus den Functionen selbst dadurch hervor, dass man die primitive Wurzel i durch ihre Potenzen ersetzt. Man wird folglich alle in Rede stehenden linearen Functionen erhalten, wenn man die $\frac{1}{2}(p+1)p$ der gegebenen primitiven Wurzel i entsprechenden Functionen nimmt und die Gruppe der $p-2$ ersten Potenzen jeder dieser Functionen bildet.

Die Formeln (31) zeigen, dass $\varDelta$ und i zu gleicher Zeit quadratische Reste oder quadratische Nichtreste von p sind; daraus geht hervor, dass die Functionen, mit denen wir uns be-

schäftigen, der ersten oder der zweiten Klasse angehören (No. 432), je nachdem die Wurzel i, auf welche sie sich beziehen, Rest oder Nichtrest von p ist. Nun ist i für die Functionen $(p-1)^{\text{ter}}$ Ordnung Nichtrest; folglich gehören diese Functionen und ihre ungeraden Potenzen zur zweiten, ihre geraden Potenzen zur ersten Klasse. Man sieht zugleich, dass

$$\tfrac{1}{4}(p+1)\,p\,(p-3)$$

unserer N_{p-1} Functionen zur ersten,

$$\tfrac{1}{4}(p+1)\,p\,(p-1)$$

zur zweiten Klasse gehören.

459. Wir wollen jetzt den Fall untersuchen, in welchem die Grösse

$$t^2 = \left(\frac{a+b'}{2}\right)^2 - (ab' - ba')$$

quadratischer Nichtrest des Moduls p ist. Dann ist die Grösse t imaginär, und damit a und b' reell seien, ist den Formeln (28) zufolge erforderlich, dass die Wurzel i selbst imaginär oder dass sie gleich -1 sei. In diesem letzteren Falle muss $n=2$ sein. Wir behaupten, dass ganz allgemein die Zahl n, welche die Ordnung der Function ϑz angiebt, gleich $p+1$, oder gleich einem Divisor von $p+1$ ist. Dies leuchtet für $n=2$ unmittelbar ein; denn 2 geht in $p+1$ auf. Wir nehmen daher an, es sei $n>2$. Setzt man

$$(33).\qquad \frac{(a+b')^2}{ab'-ba'} = 2(k+1),$$

so geht die Congruenz (26) über in

$$(34).\qquad i^2 - 2ki + 1 \equiv 0 \ (mod.\ p).$$

Die Wurzeln dieser irreductibelen Congruenz (34) können nach No. 372, Lehrsatz III durch i und i^p dargestellt werden, und da ihr Produkt der Einheit congruent ist, so hat man

$$(35).\qquad i^{p+1} \equiv 1 \ (mod,\ p);$$

i kann folglich nur dann primitive Wurzel der Congruenz (25) sein, wenn n gleich $p+1$ oder gleich einem Divisor von $p+1$ ist.

Der Congruenz (34) zufolge bezeichnet k die halbe Summe der beiden conjugirten Wurzeln i und $\frac{1}{i}$; daraus ergiebt sich, dass

$$\frac{i+1}{i-1}t = \sqrt{\frac{k+1}{k-1}t^2}$$

ist. Wir werden der im zweiten Gliede dieser Formel enthaltenen Wurzelgrösse denjenigen ihrer beiden Werthe beilegen, welcher sich in der Reihe

$$1, 2, \ldots, \frac{p-1}{2}$$

vorfindet. Ihr zweiter Werth wird sich dann auf die Wurzel $\frac{1}{i}$ beziehen, welche die Umkehrung von i ist. Dies vorausgesetzt, umfasst der vorliegende Fall keine ganzen Functionen, da t^2 quadratischer Rest von p sein würde, wenn $a' = 0$ wäre. Man kann mithin $a' = 1$ machen und erhält aus den Formeln (28)

$$(36). \quad \begin{cases} a = \sqrt{\frac{k+1}{k-1}t^2} + g\ , \ b = t^2 - g^2\ , \ a' = 1, \\ b' = \sqrt{\frac{k+1}{k-1}t^2} - g\ , \ \Delta = \frac{2t^2}{k-1}. \end{cases}$$

Diese Formeln lehren uns die der Wurzel i entsprechenden linearen Functionen kennen, wenn man g die p Werthe

$$0, 1, 2, \ldots, p-1$$

ertheilt und für t^2 der Reihe nach alle $\frac{p-1}{2}$ Nichtreste nimmt. Es entstehen auf diese Weise $\frac{1}{2}p(p-1)$ lineare Functionen n^{ter} Ordnung, die zur Wurzel i gehören. Man würde zugleich die Potenzen dieser Functionen erhalten, wenn man die Wurzel i durch ihre verschiedenen Potenzen ersetzte. Man sieht auch, dass die Anzahl aller Functionen n^{ter} Ordnung, die wir betrachten, gleich

$$\tfrac{1}{2}p(p-1)\,\varphi(n)$$

ist, wo $\varphi(n)$, wie früher, die Anzahl der primitiven Wurzeln der Congruenz (25) bezeichnet. Dieser Schluss gilt auch für den Fall $n = 2$; dann hat man nur die eine primitive Wurzel $i = -1$, welche auch $k = -1$ liefert. Die Formeln (36) lehren also $\frac{1}{2}p(p-1)$ oder $\frac{1}{2}p(p-1)\,\varphi(2)$ lineare Functionen zweiter Ordnung kennen, für welche t^2 quadratischer Nichtrest von p ist. Nimmt man $n = p+1$ an, so erhält man den Ausdruck für die Anzahl der linearen Functionen $(p+1)^{\text{ter}}$ Ordnung, nämlich

$$\tfrac{1}{2}p(p-1)\,\varphi(p+1).$$

Bezeichnet endlich N_{p+1} die Gesammtzahl der linearen Functionen, für welche t^2 quadratischer Nichtrest von p, deren Ordnung folglich ein Divisor von $p+1$ ist, so ergiebt sich

$$N_{p+1} = \tfrac{1}{2}\, p(p-1)\, \Sigma\varphi(n).$$

Nun ist der Ausdruck $\Sigma\varphi(n)$, welcher sich über alle Divisoren von $p+1$, mit Ausnahme von 1, erstreckt, gleich p, mithin

$$(37). \qquad N_{p+1} = \tfrac{1}{2}\, p^2(p-1).$$

Diese N_{p+1} linearen Functionen können in $\frac{1}{2}\,p(p-1)$ Gruppen von je p Functionen getheilt werden, welche letzteren die p ersten Potenzen einer auf eine gegebene primitive Wurzel von p bezüglichen linearen Function $(p+1)^{\text{ter}}$ Ordnung sind.

In der That werden die fraglichen N_{p+1} Functionen durch die Formeln (36) geliefert, wenn man alle Wurzeln der Congruenz (35), mit Ausnahme der Einheit, benutzt, und diese Wurzeln sind nichts Anderes, als die p ersten Potenzen einer primitiven Wurzel i. Bei Anwendung dieser primitiven Wurzel liefern nun die Formeln (36) $\frac{1}{2}\,p(p-1)$ lineare Functionen $(p+1)^{\text{ter}}$ Ordnung; ausserdem gehen die Potenzen dieser Functionen aus den Functionen selbst dadurch hervor, dass die Wurzel i durch ihre Potenzen ersetzt wird. Man erhält daher alle in Rede stehenden linearen Functionen, wenn man die $\frac{1}{2}\,p(p-1)$ Functionen nimmt, welche der Wurzel i entsprechen, und die Gruppe der p ersten Potenzen einer jeden von ihnen bildet.

Die Formeln (36) zeigen, dass die Grössen Δ und $\frac{k+1}{2}$ entweder beide quadratische Reste, oder beide Nichtreste von p sind, und zwar behaupten wir, diese Grössen seien Reste oder Nichtreste, jenachdem die Ordnung n der Function ϑz in $\frac{p+1}{2}$ aufgeht oder nicht. Man hat nämlich der Congruenz (34) zufolge

$$\frac{k+1}{2} \equiv \frac{(i+1)^2}{4i} \quad (mod.\ p).$$

Erhebt man diese Congruenz auf die Potenz $\frac{p-1}{2}$, so ergiebt sich

$$\left.\begin{aligned} \left(\frac{k+1}{2}\right)^{\frac{p-1}{2}} &\equiv \frac{(i+1)^{p-1}}{i^{\frac{p-1}{2}}} \equiv \frac{i(i+1)^p}{i^{\frac{p+1}{2}}(i+1)} \\ &\equiv \frac{i^{p+1}+i}{i^{\frac{p+1}{2}}(i+1)} \equiv \frac{1}{i^{\frac{p+1}{2}}} \end{aligned}\right\} \quad (mod.\ p).$$

Es ist aber

$$i^{\frac{p+1}{2}} \equiv +1 \text{ oder } i^{\frac{p+1}{2}} \equiv -1 \pmod{p},$$

jenachdem n in $\frac{p+1}{2}$ aufgeht oder nicht; unter den nämlichen Voraussetzungen hat man daher

$$\left(\frac{k+1}{2}\right)^{\frac{p-1}{2}} \equiv +1 \text{ oder } \left(\frac{k+1}{2}\right)^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

d. h.

$$\Delta^{\frac{p-1}{2}} \equiv +1 \text{ oder } \Delta^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Daraus geht hervor, dass die linearen Functionen $(p+1)^{\text{ter}}$ Ordnung und die ungeraden Potenzen derselben der zweiten, die geraden Potenzen aber der ersten Klasse angehören. Unter unseren N_{p+1} Functionen giebt es also

$$\tfrac{1}{4}\, p(p-1)^2$$

Functionen erster,

$$\tfrac{1}{4}\,(p+1)\; p(p-1)$$

Functionen zweiter Art.

460. Addirt man die Einheit und die drei Zahlen N_p, N_{p-1}, N_{p+1}, so muss man wieder die Anzahl N aller in Beziehung auf den Modul p genommenen linearen Functionen erhalten. In der That lässt sich mittels der Formeln (4), (21), (32) und (37) bewahrheiten, dass

$$N = 1 + N_p + N_{p-1} + N_{p+1}$$

ist. Bezeichnet ausserdem G die Anzahl der verschiedenen Gruppen, welche aus den Potenzen einer linearen Function der Ordnung p, $p-1$ oder $p+1$ bestehen, so überzeugt man sich leicht von der Richtigkeit der Formel

$$G = p^2 + p + 1.$$

Besondere Beachtung verdienen die Functionen zweiter Ordnung, welche sich in die beiden oben unterschiedenen Klassen vertheilen. Dieselben sind theils die $\left(\frac{p-1}{2}\right)^{\text{ten}}$ Potenzen der Functionen $(p-1)^{\text{ter}}$ Ordnung, theils die $\left(\frac{p+1}{2}\right)^{\text{ten}}$ Potenzen der Functionen $(p+1)^{\text{ter}}$ Ordnung. Die ersteren, deren Anzahl gleich $\frac{1}{2}\,p(p+1)$ ist, gehören der ersten oder der zweiten Klasse an, je nachdem $\frac{p-1}{2}$ gerade oder ungerade, d. h. je nachdem p

von der Form $4q + 1$ oder von der Form $4q + 3$ ist. Die Anzahl der letzteren ist $\frac{1}{2}p(p-1)$; dieselben gehören zur ersten oder zur zweiten Klasse, je nachdem $\frac{p+1}{2}$ gerade oder ungerade, d. h. je nachdem p von der Form $4q + 3$, oder von der Form $4q + 1$ ist. Wie man sieht, giebt es im Ganzen p^2 Functionen zweiter Ordnung. In diesem Falle $n = 2$, in welchem man $i = -1$ hat, reducirt sich die Congruenz (26) auf $a + b' \equiv 0$ (*mod.* p), und der allgemeine Ausdruck der Functionen zweiter Ordnung ist somit

$$\vartheta z = \frac{az + b}{a'z - a}.$$

Zu demselben Resultat führt die Formel (10), da eine Function zweiter Ordnung ihrer Umkehrung gleich ist.

461. Aus den vorstehenden Entwicklungen ist ersichtlich, dass zur Bildung der verschiedenen Gruppen, welche die Potenzen ein und derselben nach dem Primzahlmodul p genommenen linearen Function enthalten, die Kenntniss einer primitiven Wurzel jeder der Congruenzen

$$i^{p-1} \equiv 1\ ,\ i^{p+1} \equiv 1\ (mod.\ p)$$

genügt. Die Wurzeln der ersteren Congruenz sind nichts Anderes, als die primitiven Wurzeln der Primzahl p, und in No. 372 hat man gesehen, wie man die primitiven Wurzeln der zweiten Congruenz bestimmen kann. Will man z. B. die linearen Functionen $(p + 1)^{\text{ter}}$ Ordnung für die Moduln 5, 7, 11 bilden, so genügt es, für jeden dieser Moduln einen Werth von k zu ermitteln. Nun sind die primitiven Wurzeln i für diese verschiedenen Fälle durch die Congruenzen

$$\frac{(i^6-1)\ (i-1)}{(i^3-1)\ (i^2-1)} \equiv 0\ (mod.\ 5),$$

$$\frac{i^8-1}{i^4-1} \equiv 0\ (mod.\ 7),$$

$$\frac{(i^{12}-1)\ (i^2-1)}{(i^6-1)\ (i^4-1)} \equiv 0\ (mod.\ 11),$$

oder

$$i^2 - i + 1 \equiv 0\ (mod.\ 5),$$

$$i^2 \pm 4i + 1 \equiv 0\ (mod.\ 7),$$

$$i^2 \pm 6i + 1 \equiv 0\ (mod.\ 11)$$

gegeben; es ist folglich $k = 2$ für den Modul 5, $k = \pm 2$ für den Modul 7, und $k = \pm 3$ für den Modul 11.

Analytische Functionen, welche geeignet sind, die Substitutionen darzustellen.

462. In den meisten Fällen, in denen man die Substitutionen mehrerer gegebenen Grössen zu betrachten hat, empfiehlt es sich, diese Grössen durch ein und denselben Buchstaben darzustellen, und diesen Buchstaben mit einem veränderlichen Index z zu versehen, der so viele von einander verschiedene Werthe anzunehmen vermag, als Grössen gegeben sind. Dann beziehen sich die Substitutionen, die man auszuführen hat, auf die Indices.

Wir ertheilen z der Reihe nach die n Werthe, welche dieser Index erhalten kann, und setzen voraus, dieselben stimmten, abgesehen von der Reihenfolge, mit den Werthen überein, welche eine gegebene Function $f(z)$ von z zu gleicher Zeit annimmt. Dann wird man an den gegebenen Grössen eine gewisse Substitution dadurch vollziehen, dass man jeden Index z durch $f(z)$ ersetzt. Diese Substitution kann durch

$$\begin{bmatrix} f(z) \\ z \end{bmatrix},$$

oder einfacher durch $f(z)$ dargestellt werden. Auf diese Weise lässt sich jede Substitution analytisch durch eine Function darstellen. Nehmen wir z. B. an, die Werthe des Index z seien die n Zahlen

$$0, 1, 2, \ldots, (n-1),$$

und es seien

$$a, b, c, \ldots, k$$

eben dieselben Zahlen in einer andern Reihenfolge; setzt man der Kürze wegen

$$F(z) = z(z-1)(z-2)\ldots(z-n+1),$$

und bezeichnet die Abgeleitete von $F(z)$ mit $F'(z)$, so wird die ganze Function

$$f(z) = \frac{aF(z)}{zF'(0)} + \frac{bF(z)}{(z-1)F'(1)} + \cdots + \frac{kF(z)}{(z-n+1)F'(n-1)}$$

die Werthe $a, b, c, \ldots, k$ annehmen, wenn man z die Werthe $0, 1, 2, \ldots, (n-1)$ beilegt; diese Function wird somit eine Substitution darstellen können.

463. Wenn die Anzahl n der gegebenen Grössen gleich

einer Primzahl p ist, so ist es oft zweckmässig, ein System von irgend welchen p nach dem Modul p incongruenten ganzen Zahlen als Indices zu nehmen und zwei nach dem Modul congruente Zahlen ohne Unterschied denselben Index darstellen zu lassen. Dann reducirt sich die in der vorigen Nummer mit $F(z)$ bezeichnete Function auf

$$F(z) \equiv z^p - z,$$

und man hat

$$F'(z) \equiv -1 \ (mod.\ p).$$

Zugleich geht der Ausdruck der ganzen Functionen $f(z)$, welche geeignet sind, die Substitutionen darzustellen, über in

$$f(z) \equiv -\frac{a(z^p - z)}{z} - \frac{b(z^p - z)}{z-1} - \cdots - \frac{k(z^p - z)}{z-p+1} \ (mod.\ p),$$

oder, wenn man die angedeuteten Divisionen ausführt, in

$$\left.\begin{array}{l} f(z) \equiv -a(z^{p-1} - 1) - b(z^{p-1} + z^{p-2} + \cdots + z) \\ \qquad - c(z^{p-1} + 2z^{p-2} + \cdots + 2^{p-2} z) \ \ldots . \\ \qquad - k\left[z^{p-1} + (p-1)z^{p-2} + \cdots + (p-1)^{p-2} z\right] \end{array}\right\} (mod.\ p).$$

Ordnet man diese Congruenz nach Potenzen von z, so folgt, da

$$a + b + c + \cdots + k \equiv 0 \ (mod.\ p)$$

ist,

$$\left.\begin{array}{l} f(z) \equiv a - \left[b + 2^{p-2}c + \cdots + (p-1)^{p-2}k\right]z \\ \qquad - \left[b + 2^{p-3}c + \cdots + (p-1)^{p-3}k\right]z^2 \\ \qquad - \ldots\ldots\ldots\ldots\ldots\ldots \\ \qquad - \left[b + 2c \quad + \cdots + (p-1)k \quad\right]z^{p-2} \end{array}\right\} (mod.\ p).$$

464. Im 57ten Bande der Comptes rendus de l'Académie des Sciences hat Hermite den Beweis geführt, dass die Polynome $f(z)$, deren Ausdruck wir soeben gegeben haben, eine Eigenschaft besitzen, die dazu dienen kann, sie zu charakterisiren. Es besteht nämlich der folgende Satz:

Lehrsatz. — Es sei $f(z)$ eine ganze Function von z, deren Grad $p-2$ und deren Coefficienten ganze Zahlen sind; ferner sei $f_m(z)$ die ganze Function, welche man erhält, wenn man mittels der Congruenz $z^p \equiv z$ $(mod.\ p)$ den Grad der $m$ten Potenz des Polynoms $f(z)$ kleiner als p macht. Damit dann die Function $f(z)$ geeignet sei, eine Substitution von p nach dem Primzahlmodul p incongruenten Indices darzustellen, ist er-

forderlich und hinreichend, dass der Coefficient von z^{p-1} in jeder der Functionen

$$f_2(z)\,,\ f_3(z)\,,\ \ldots\,,\ f_{p-2}(z)$$

nach dem Modul p der Null congruent sei.

Es sei

$$(1).\quad f(z) = A_0 + A_1 z + A_2 z^2 + \cdots + A_{p-2} z^{p-2}.$$

Erheben wir dieses Polynom auf die m^{te} Potenz und reduciren sodann mittels der Congruenz

$$z^p \equiv z\ (mod.\ p),$$

so erhalten wir ein Resultat von der Form

$$(2).\quad [f(z)]^m \equiv f_m(z) \equiv A_0^{(m)} + A_1^{(m)} z + \cdots + A_{p-1}^{(m)} z^{p-1}\ (mod.\ p).$$

Ausserdem setzen wir

$$(3).\qquad [f(0)]^m + [f(1)]^m + \cdots + [f(p-1)]^m = S_m\,.$$

Ertheilt man z in der Formel (2) die Werthe

$$0\,,\ 1\,,\ 2\,,\ 3\,,\ \ldots\,,\ (p-1)$$

und addirt die Resultate, so folgt

$$(4).\qquad S_m \equiv -\,A_{p-1}^{(m)}\ (mod.\ p);$$

denn z^{p-1} ist $\equiv 0$ oder $\equiv 1$, je nachdem z Null oder von Null verschieden ist, und die Summe $1^\mu + 2^\mu + \cdots + (p-1)^\mu$ ist $\equiv 0$, wenn μ kleiner als $p-1$ ist.

Dies vorausgesetzt, nehmen wir an, $f(z)$ sei geeignet, eine Substitution darzustellen. Dann reducirt sich die Formel (3) auf

$$0^m + 1^m + 2^m + \cdots + (p-1)^m = S_m\,,$$

und folglich ist S_m für alle Werthe von m, die kleiner als $p-1$ sind, nach dem Modul p der Null congruent; man hat also der Formel (4) zufolge

$$(5).\qquad A_{p-1}^{(m)} \equiv 0\ (mod.\ p).$$

Zweitens setzen wir voraus, die Function $f(z)$ sei so beschaffen, dass die Congruenz (5) für die Werthe $2\,,\ 3\,,\ \ldots\,,\ (p-2)$ von m stattfinde. Der Formel (4) wegen ist für dieselben Werthe von m

$$S_m \equiv 0\ (mod.\ p).$$

Diese Congruenz bleibt nach (1) auch für $m = 1$ bestehen; ebenso behält sie ihre Gültigkeit für $m = p$, da für jedes beliebige

$z\, z^p \equiv z$ ist. Mit Rücksicht auf die Newtonschen Formeln ergiebt sich dann, dass die Congruenz

$$[Z - f(0)]\ [Z - f(1)] \ldots [Z - f(p-1)] \equiv 0 \pmod{p}$$

die Form

$$Z^p - \alpha Z \equiv 0 \pmod{p},$$

oder sogar die Form

$$Z^p - Z \equiv 0 \pmod{p}$$

hat. Jeder von 1 oder 0 verschiedene Werth von α würde nämlich nur eine einzige der Null gleiche reelle Wurzel Z bestehen lassen, und der Werth $\alpha = 0$ würde p der Null gleiche Wurzeln liefern, was deshalb unzulässig ist, weil die Congruenz

$$f(z) \equiv 0 \pmod{p}$$

vom Grade $p - 2$ ist, also nicht mehr als $p - 2$ Wurzeln besitzen kann.

Daraus geht hervor, dass, wenn man z die Werthe

$$0\,,\,1\,,\,2\,,\,\ldots\,,\,(p-1)$$

beilegt, die Function $f(z)$ ebendieselben Werthe, nur in einer möglicherweise anderen Reihenfolge, annimmt; $f(z)$ ist daher geeignet, eine Substitution darzustellen.

465. Wenn die ganze Function $f(z)$ eine Substitution von p nach dem Primzahlmodul p incongruenten Indices darstellt, so wird offenbar auch die Function

$$\vartheta z = \alpha f(z + \beta) + \gamma$$

eine Substitution darstellen. Man kann nun über die unbestimmte Grösse α in der Weise verfügen, dass der Coefficient der höchsten Potenz von z gleich Eins werde. Sodann gestattet es die Unbestimmtheit von β, die zweithöchste Potenz von z zum Verschwinden zu bringen. Endlich kann man die Grösse γ so wählen, dass der von z unabhängige Term wegfällt. Die Function ϑz hat dann die Form

$$\vartheta z = a_1 z + a_2 z^2 + \cdots + a_{\nu-2} z^{\nu-2} + z^\nu,$$

und darin ist ν gleich $p - 2$ oder kleiner als $p - 2$.

Die Substitutionen von der Form ϑz sind von Hermite reducirte Substitutionen genannt worden. Es ist klar, dass man noch allgemeinere Substitutionen $f(z)$ erhält, wenn man

$$f(z) = \alpha\vartheta(z+\beta) + \gamma$$

setzt, worin α, β, γ unbestimmte Grössen bezeichnen. Man beachte, dass die reducirten Substitutionen den Index Null nicht versetzen.

Der Lehrsatz der No. 464 nimmt eine einfachere Form an, wenn man ihn auf die reducirten Functionen anwendet. Erhebt man nämlich die Function ϑz auf die m^{te} Potenz und reducirt sodann mittels der Congruenz $z^p \equiv z \pmod{p}$, so wird man keinen von z unabhängigen Term einführen; ersetzt man daher z^{p-1} durch 1, so wird der Coefficient von z^{p-1} der von z unabhängige Term werden. Man kann dann den oben bewiesenen Satz folgendermassen aussprechen:

Damit die reducirte Function ϑz eine Substitution darstellen könne, ist erforderlich und hinreichend, dass wenn man ϑz auf die Potenzen $2, 3, \ldots, (p-2)$ erhebt und die Resultate mittels der Congruenz $z^{p-1} \equiv 1 \pmod{p}$ reducirt, die von z unabhängigen Terme der Null congruent seien.

Die reducirten Functionen ϑz sind noch einer weiteren Reduction fähig. Setzt man nämlich

$$\Theta(z) = a\vartheta(\alpha z),$$

so kann man über die unbestimmte Grösse α so verfügen, dass der Coefficient der höchsten Potenz von z in $\Theta(z)$ gleich 1 werde. Es bleibt dann noch eine unbestimmte Grösse a übrig, die man nach Belieben wählen kann. Diese Betrachtungen werden weiterhin ihre Anwendung finden.

466. Wenn die Anzahl n der gegebenen Grössen gleich einer Potenz p^ν einer Primzahl p ist, so kann man mit Galois die p^ν Werthe als Indices wählen, welche der Ausdruck

$$a_0 + a_1 i + a_2 i^2 + \cdots + a_{\nu-1} i^{\nu-1}$$

annehmen kann, wenn i eine Wurzel einer irreductibelen Congruenz ν^{ten} Grades

$$F(x) \equiv 0 \pmod{p}$$

bezeichnet. Wenn die irreductibele Function $F(x)$ zum Exponenten $p^\nu - 1$ gehört, so ist i eine primitive Wurzel für die Congruenz

$$x^{p^\nu - 1} - 1 \equiv 0 \pmod{p},$$

und die Indices, Null ausgenommen, werden durch die Potenzen

$$i\ ,\ i^2\ ,\ \ldots\ ,\ i^{p^\nu-1}$$

dargestellt.

Hat man endlich

$$n = p^\nu q^\mu r^\lambda \ldots,$$

wo $p\ ,\ q\ ,\ r\ ,\ \ldots$ ungleiche Primzahlen und $\nu\ ,\ \mu\ ,\ \lambda\ ,\ \ldots$ irgendwelche Exponenten bezeichnen, so kann es vortheilhaft sein, die gegebenen Grössen durch einen einzigen Buchstaben darzustellen, welchem man mehrere Indices $\alpha\ ,\ \beta\ ,\ \gamma\ ,\ \ldots$ anhängt, deren Anzahl gleich der Anzahl der Primzahlen $p, q, r, \ldots$ ist, und als Werthe der Indices die ganzen Functionen zu nehmen, welche beziehungsweise aus einer Wurzel der Congruenzen

$$F_1(x) \equiv 0\ (mod.\ p),$$
$$F_2(x) \equiv 0\ (mod.\ q),$$
$$F_3(x) \equiv 0\ (mod.\ r),$$
$$\ldots\ldots\ldots\ldots$$

zusammengesetzt sind; $F_1(x)\ ,\ F_2(x)\ ,\ F_3(x)\ ,\ \ldots\ ,$ bezeichnen ganze Functionen der Grade $\nu\ ,\ \mu\ ,\ \lambda\ ,\ \ldots\ ,$ welche in Beziehung auf ihre respectiven Moduln $p\ ,\ q\ ,\ r\ ,\ \ldots$ irreductibel sind.

Rationale und lineare Substitutionen.

467. Die in Beziehung auf den Primzahlmodul p genommenen ganzen und linearen Functionen $az + b$ liefern Substitutionen der p Indices

$$0\ ,\ 1\ ,\ 2\ ,\ \ldots\ ,\ (p-1).$$

Die Gesammtzahl dieser Substitutionen ist $p(p-1)$, und es liegt auf der Hand, dass dieselben ein conjugirtes System bilden.

Die in Beziehung auf den Primzahlmodul p genommenen rationalen Functionen der Form

$$(1).\qquad \vartheta z = \frac{az + b}{a'z + b'}$$

können dazu benutzt werden, Substitutionen von $p+1$ Indices darzustellen; die Werthe, welche man diesen Indices beilegen muss, sind dann

$$0\ ,\ 1\ ,\ 2\ ,\ \ldots\ ,\ (p-1)\ ,\ \infty,$$

und man hat zwei nach dem Modul p congruente Zahlen immer als zur Darstellung desselben Index geeignet anzusehen. Die Ein-

setzung von ∞ an die Stelle von z erfolgt nach den Regeln der gemeinen Algebra, und wenn der Nenner von ϑz für einen besonderen Werth von z der Null congruent ist, so nimmt die Function den Werth ∞ an. Es ist das eine Uebereinkunft, die man treffen kann, vorausgesetzt, dass sie nicht mit einem der Fundamental-Sätze der Theorie der Congruenzen in Widerspruch steht.

Löst man die Formel (1) nach z auf, so folgt

$$z = \frac{b - b'\vartheta z}{a'\vartheta z - a}.$$

Diese Formel zeigt, dass es nur einen Werth von z giebt, der geeignet ist, ϑz einen gegebenen Werth annehmen zu lassen, was nöthig ist, damit ϑz eine Substitution darstellen könne.

Die Congruenz

$$(2). \qquad \vartheta z \equiv z \ (mod.\ p)$$

lässt sich auf die Form

$$(3). \qquad a'z^2 - (a - b')z - b \equiv 0 \ (mod.\ p),$$

oder

$$[2a'z - (a - b')]^2 \equiv (a + b')^2 - 4\,(ab' - ba') \ (mod.\ p)$$

bringen. Keine ihrer Wurzeln wird reell sein, wenn die Grösse

$$(4). \qquad (a + b')^2 - 4\,(ab' - ba')$$

quadratischer Nichtrest von p ist. Da dann die Congruenz (2) für keinen Werth von z bestehen kann, so versetzt die Substitution ϑz alle Indices. Wenn die Grösse (4) der Null congruent ist, so hat die Congruenz (2) oder (3) zwei reelle und gleiche Wurzeln; folglich versetzt die Substitution ϑz p Indices. Wenn endlich der Ausdruck (4) quadratischer Rest von p ist, so hat die Congruenz (2) zwei reelle und ungleiche Wurzeln; die Substitution ϑz versetzt somit nur $p - 1$ Indices.

468. Wir bezeichnen mit n die Ordnung der linearen Function ϑz und betrachten die Reihe

$$z, \vartheta z, \vartheta^2 z, \ldots, \vartheta^{n-1} z.$$

Wenn die Congruenz $\vartheta z \equiv z$ $(mod.\ p)$ eine reelle Wurzel z_0 hat, so werden die Terme dieser Reihe sich für $z = z_0$ sämmtlich auf z_0 reduciren; für jeden anderen Werth z_1 von z aber wird keiner dieser Terme gleich z_0 werden. Die etwa vorhandenen Werthe z_0 bei Seite lassend, behaupten wir, dass die Terme der

vorhergehenden Reihe immer verschiedene Werthe haben werden. Hätte man z. B.

$$\vartheta^{\mu+\nu} z_1 \equiv \vartheta^{\mu} z_1 \ (mod.\ p),$$

so würde sich, wenn man

$$z_2 = \vartheta^{\mu} z_1$$

setzte,

$$\vartheta^{\nu} z_2 \equiv z_2 \ (mod.\ p)$$

ergeben. Dies ist unmöglich; da nämlich ν kleiner als n ist, so kann man nicht identisch

$$\vartheta^{\nu} z \equiv z \ (mod.\ p)$$

haben; ausserdem ist die letzte Congruenz den Formeln der No. 455 zufolge nichts Anderes, als

$$\vartheta z \equiv z \ (mod.\ p),$$

und lässt daher die Wurzel z_2 nicht zu.

Wir können daraus den Schluss ziehen, dass die lineare Function ϑz eine Substitution n^{ter} Ordnung darstellt, und nach der Eintheilung, die wir begründet haben, sieht man, dass das System der linearen Substitutionen nur cyclische Substitutionen, deren Ordnung eine der Zahlen $p+1$, p, $p-1$ ist, nebst den Potenzen eben derselben Substitutionen umfasst.

Die Gesammtzahl der linearen Substitutionen ist $(p+1)p(p-1)$, und darunter befinden sich $\frac{(p+1)\,p(p-1)}{2}$, deren Determinante quadratischer Rest des Moduls ist. Daraus ergiebt sich der folgende Satz:

Lehrsatz. — Die Gesammtheit aller auf einen Primzahlmodul p bezogenen linearen Substitutionen macht ein 3 mal transitives conjugirtes System der Ordnung $(p+1)\,p(p-1)$ aus. Ausserdem bilden die linearen Substitutionen, deren Determinante ein quadratischer Rest des Moduls ist, ein zweimal transitives conjugirtes System der Ordnung $\frac{1}{2}(p+1)p(p-1)$.

Das erste dieser Systeme umfasst nämlich cyclische Substitutionen der Ordnung $p+1$, der Ordnung p und der Ordnung $p-1$. Was das zweite System betrifft, so enthält es cyclische Substitutionen der Ordnung p, nebst regelmässigen Substitutionen der Ordnung $\frac{p\pm 1}{2}$, und unter diesen letzteren kann man stets

eine finden, welche einen gegebenen Index z_0 durch einen anderen gegebenen Index z_1 ersetzt.

Im Falle $p = 5$ erhält man sofort wieder das 3 mal transitive System, das aus Substitutionen von 6 Buchstaben besteht, und mit dem wir uns in No. 440 beschäftigt haben.

Ueber einige Eigenschaften der linearen Substitutionen.

469. Lehrsatz I. — Bezeichnet Ez allgemein die $p(p-1)$ nach dem Modul p genommenen linearen und ganzen Substitutionen und φz irgend eine gegebene lineare Function, so bilden die Substitutionen von der Form $\varphi^{-1} E \varphi z$ ein conjugirtes System der Ordnung $p(p-1)$; auch lassen sie den Index z, für welchen die Function $\varphi(z)$ unendlich ist, unversetzt.

Erstens bilden die Substitutionen $\varphi^{-1} E \varphi z$ ein conjugirtes System, welches demjenigen der Substitutionen Ez ähnlich ist (No. 415). Was die zweite Behauptung betrifft, so sei z_0 der Index, welchen die Substitutionen $\varphi^{-1} E \varphi z$ nicht versetzen; dann ist

$$\varphi^{-1} E \varphi z_0 \equiv z_0 \ (mod.\ p),$$

mithin

$$E \varphi z_0 \equiv \varphi z_0 \ (mod.\ p).$$

Daraus geht hervor, dass die Substitutionen Ez den Index φz_0 nicht versetzen; man hat daher

$$\varphi z_0 = \infty.$$

Zusatz I. — Es giebt $p + 1$ conjugirte Systeme der Ordnung $p(p-1)$, deren jedes aus linearen Substitutionen zusammengesetzt ist, welche sämmtlich ein und denselben Index nicht versetzen.

Zusatz II. — Jedes System der Ordnung $p(p-1)$ wird durch Multiplication der beiden Systeme erhalten, welche beziehungsweise aus den Potenzen zweier linearen Substitutionen zusammengesetzt sind, die ein und denselben Index z_0 nicht versetzen und von denen die eine die Ordnung p, die andere die Ordnung $p-1$ hat.

Es seien nämlich

$$z\,,\ \vartheta z\,,\ \vartheta^2 z\,,\ \ldots\,,\ \vartheta^{p-2} z\,;\ \vartheta^{p-1} z\,,$$
$$z\,,\ \varphi z\,,\ \varphi^2 z\,,\ \ldots\,,\ \varphi^{p-2} z$$

die Systeme, welche aus den Potenzen von ϑz und von φz bestehen; diese Substitutionen, deren Ordnungen beziehungsweise p und $p-1$ sind, lassen einen Index z_0 unversetzt. Da die Anzahl der Produkte $\varphi^\mu \vartheta^\nu z$ gleich $p(p-1)$ ist, so haben wir nur die Verschiedenheit derselben nachzuweisen. Hätte man nun

$$\varphi^\mu \vartheta^\nu z = \varphi^{\mu'} \vartheta^{\nu'} z\,,$$

so würde sich

$$\varphi^{\mu-\mu'} z = \vartheta^{\nu'-\nu} z$$

ergeben, und dies erfordert, dass $\mu' = \mu$, $\nu' = \nu$ sei, da die Substitution $(p-1)^{\text{ter}}$ Ordnung φz zwei Indices unversetzt lässt, während ϑz p Indices versetzt. Unser Satz ist somit bewiesen.

Zusatz III. — Das System der $(p+1)\,p(p-1)$ linearen Substitutionen wird durch Multiplication eines der Systeme der Ordnung $p(p-1)$, dessen Substitutionen einen Index unversetzt lassen, mit dem Systeme der Potenzen einer linearen Substitution der Ordnung $p+1$ erhalten.

Es seien

$$z\,,\ \varphi_1 z\,,\ \varphi_2 z\,,\ \ldots\,,\ \varphi_{p(p-1)-1} z$$

und

$$z\,,\ \vartheta z\,,\ \vartheta^2 z\,,\ \ldots\,,\ \vartheta^p z$$

die beiden in Rede stehenden Systeme. Da die Anzahl der Produkte $\varphi_\mu \vartheta^\nu z$ gleich $(p+1)\,p(p-1)$ ist, so genügt es ihre Verschiedenheit nachzuweisen. Wenn nun nicht μ' und ν' beziehungsweise gleich μ und ν sind, so kann man nicht

$$\varphi_{\mu'} \vartheta^{\nu'} z = \varphi_\mu \vartheta^\nu z$$

haben; denn daraus würde

$$\varphi_\mu^{-1} \varphi_{\mu'} z = \vartheta^{\nu-\nu'} z$$

folgen, und dies ist unmöglich, da die Substitution ϑ einen Index versetzt, welchen die Substitutionen φ unversetzt lassen.

470. Lehrsatz II. — Es seien ϑz eine lineare Substitution der Ordnung p, welche den Index z_0 nicht versetzt, und φz irgend eine lineare Substitution. Damit

$$\varphi^{-1}\vartheta\varphi z = \vartheta^\mu z$$

sein könne, ist erforderlich und hinreichend, dass die Substitution φz den Index z_0 nicht versetze.

Die Congruenz

$$\vartheta z_0 \equiv z_0 \ (mod.\ p)$$

zieht

$$\vartheta^\mu z_0 \equiv z_0 \ (mod.\ p)$$

nach sich. Hat man daher

$$\vartheta\varphi z = \varphi\vartheta^\mu z,$$

so ergiebt sich für $z = z_0$

$$\vartheta\varphi z_0 \equiv \varphi z_0 \ (mod.\ p),$$

und da die Substitution ϑz alle Indices, mit Ausnahme von z_0, versetzt, so ist

$$\varphi z_0 \equiv z_0 \ (mod.\ p);$$

dies drückt aus, dass die Substitution φz z_0 unversetzt lässt.

Wenn umgekehrt φz den Index z_0 nicht versetzt, so gilt dasselbe von der Substitution $\varphi^{-1}\vartheta\varphi z$; diese ist ausserdem von derselben Ordnung wie ϑz. Folglich haben die beiden Congruenzen

$$\vartheta z \equiv z\ ,\ \varphi^{-1}\vartheta\varphi z \equiv z \ (mod.\ p)$$

nur die Wurzel z_0. Nach der Bildungsweise der linearen Functionen folgt daraus, dass die Functionen $\varphi^{-1}\vartheta\varphi z$ und ϑz ein und derselben Gruppe von Potenzen angehören, und man hat

$$\varphi^{-1}\vartheta\varphi z = \vartheta^\mu z.$$

Es ist zu beachten, dass die Ordnung n von φz gleich p oder gleich einem Divisor von $p - 1$ ist. Wenn aber der erstere Fall stattfindet, so ist φz nichts Anderes, als eine Potenz von ϑz.

Zusatz I. — Eine lineare Substitution p^{ter} Ordnung ist gegen keine andere lineare Substitution vertauschbar, die nicht eine ihrer Potenzen ist.

Wenn nämlich die Substitution ϑz von der Ordnung p, und wenn φz keine Potenz von ϑz ist, so erfordert die Gleichung

$$(1).\qquad \vartheta\varphi z = \varphi\vartheta z \text{ oder } \varphi^{-1}\vartheta\varphi z = \vartheta z,$$

wie wir soeben bemerkt haben, dass die Ordnung von φz ein Divisor von $p - 1$ sei. Dann hat die Congruenz

$$(2).\qquad \varphi z \equiv z \ (mod.\ p)$$

eine von z_0 verschiedene Wurzel z_1, und die Gleichung (1) liefert für $z = z_1$

$$\vartheta z_1 \equiv \varphi \vartheta z_1 \ (mod.\ p),$$

woraus hervorgeht, dass ϑz_1 eine Wurzel der Congruenz (2) ist. Die Wurzeln dieser Congruenz sind nun z_1 und $z_0 = \vartheta z_0$; man müsste daher

$$\vartheta z_1 \equiv z_1 \text{ oder } \vartheta z_1 \equiv \vartheta z_0,$$

und folglich $z_1 = z_0$ haben, was nicht der Fall ist.

Zusatz II. — Es seien ϑz eine lineare Substitution der Ordnung p und φz eine lineare Substitution, deren Ordnung n ein Divisor von $p - 1$ ist. Wenn ϑz und φz ein und denselben Index z_0 unversetzt lassen, so erhält man durch Multiplication des Systems der Potenzen von ϑz mit demjenigen der Potenzen von φz ein System conjugirter Substitutionen der Ordnung np. Dieses System der Ordnung np enthält ausserdem alle linearen Substitutionen n^{ter} Ordnung, welche den Index z_0 nicht versetzen.

Es liegt auf der Hand, dass man ein conjugirtes System der Ordnung np erhält, wenn man die beiden Systeme

$$z,\ \vartheta z,\ \vartheta^2 z,\ \ldots,\ \vartheta^{p-1} z,$$
$$z,\ \varphi z,\ \varphi^2 z,\ \ldots,\ \varphi^{n-1} z$$

in einander multiplicirt. Ausserdem enthält dieses System der Ordnung np alle Substitutionen n^{ter} Ordnung von der Form $\vartheta^{-i}\varphi\vartheta^i z$, und da i irgend einen der Werthe

$$0,\ 1,\ 2,\ 3,\ \ldots,\ (p-1)$$

haben kann, so findet man p Systeme, deren jedes aus den Potenzen einer Substitution n^{ter} Ordnung gebildet ist, welche den Index z_0 nicht versetzt. Eine grössere Anzahl solcher Systeme giebt es nicht; wir haben daher nur zu zeigen, dass die eben besprochenen Systeme von einander verschieden sind. In der That behaupten wir, es könne nicht

$$\vartheta^{-i}\varphi\vartheta^i z = \vartheta^{-i-j}\varphi^k\vartheta^{i+j} z$$

sein. Wäre dies nämlich der Fall, so würde sich

$$\vartheta^j\varphi\vartheta^{-j} z = \varphi^k z$$

ergeben. Man hat aber $\varphi^{-1}\vartheta\varphi z = \vartheta^\mu z$, und folglich

$$\varphi^{-1}\vartheta^{j}\varphi z = \vartheta^{\mu j} z \ , \ \vartheta^{j}\varphi z = \varphi\vartheta^{\mu j} z;$$

es würde somit

$$\varphi\vartheta^{(\mu-1)j} z = \varphi^{k} z \ , \ \vartheta^{(\mu-1)j} z = \varphi^{k-1} z$$

sein, und dies erfordert, dass $k = 1$, $\mu \doteq 1$ sei. Hätte man aber $\mu = 1$, so wären die Substitutionen ϑz und φz gegen einander vertauschbar, was nicht der Fall ist.

471. Lehrsatz III. — *Es seien ϑz eine lineare Substitution der Ordnung $p \pm 1$ und φz eine von den Potenzen von ϑz verschiedene lineare Substitution. Damit*

$$\varphi^{-1}\vartheta\varphi z = \vartheta^{\mu} z \tag{1}$$

sein könne, ist erforderlich und hinreichend, dass φz eine Substitution zweiter Ordnung sei, und dass die reellen oder imaginären Wurzeln z_0, z_1 der Congruenz

$$\vartheta z \equiv z \ (mod.\ p)$$

so beschaffen seien, dass man

$$\varphi z_0 \equiv z_1 \ , \ \varphi z_1 \equiv z_0 \ (mod.\ p)$$

habe. Falls die Ordnung von ϑz gleich $p - 1$ ist, so sind die Wurzeln z_0, z_1 reell, und die letzte Bedingung drückt aus, dass die Substitution φz die beiden Indices transponirt, welche ϑz nicht versetzt.

Wenn die Gleichung (1) stattfindet, so fällt das System der Potenzen von $\varphi^{-1}\vartheta\varphi z$, nämlich

$$z \ , \ \varphi^{-1}\vartheta\varphi z \ , \ \varphi^{-1}\vartheta^{2}\varphi z, \ \ldots \tag{2}$$

mit dem Systeme der Potenzen von ϑz

$$z \ , \ \vartheta z \ , \ \vartheta^{2} z, \ \ldots \tag{3}$$

zusammen. Jedes der Systeme (2) und (3) enthält eine Substitution zweiter Ordnung, und diese beiden Substitutionen müssen unter der gemachten Voraussetzung einander gleich sein; man hat also

$$\varphi^{-1}\vartheta^{\frac{p\pm1}{2}}\varphi z = \vartheta^{\frac{p\pm1}{2}} z \text{ oder } \vartheta^{\frac{p\pm1}{2}}\varphi z = \varphi\vartheta^{\frac{p\pm1}{2}} z. \tag{4}$$

Wenn umgekehrt diese Gleichung (4) besteht, so müssen die Systeme (2) und (3) zusammenfallen; denn sie sind beide von derselben Ordnung $p \pm 1$ und haben eine Substitution gemeinschaftlich.

Ersetzt man z durch $\vartheta^{\frac{p\pm 1}{2}}\varphi z$, so geht (4) über in

$$\vartheta^{\frac{p\pm 1}{2}}\varphi\vartheta^{\frac{p\pm 1}{2}}\varphi z \doteq \varphi\vartheta^{p\pm 1}\varphi z = \varphi^2 z;$$

$\vartheta^{\frac{p\pm 1}{2}}\varphi z$ und φz haben daher dasselbe Quadrat; daraus geht hervor, dass diese Functionen von der zweiten Ordnung sind. Wäre nämlich das Gegentheil der Fall, so würden die in Rede stehenden Substitutionen beide der Gruppe der Potenzen ein und derselben linearen Substitution $\psi(z)$ angehören; man hätte dann

$$\vartheta^{\frac{p\pm 1}{2}}\varphi z = \psi^\mu z\ ,\ \varphi z = \psi^\nu z,$$

mithin

$$\vartheta^{\frac{p\pm 1}{2}} z \equiv \psi^{\mu-\nu} z,$$

und folglich würden die Functionen φ und ϑ sich in derselben Gruppe von Potenzen vorfinden, was der Voraussetzung widerspricht. Man hat also

$$(5).\qquad \varphi^2 z = z\ ,\ \vartheta^{\frac{p\pm 1}{2}}\varphi\vartheta^{\frac{p\pm 1}{2}}\varphi z = z,$$

und umgekehrt ziehen diese Gleichungen die Formel (4) nach sich.

Dies vorausgesetzt, seien z_0 und z_1 die reellen oder imaginären Wurzeln der Congruenzen

$$\vartheta z \equiv z\ ,\ \vartheta^{\frac{p\pm 1}{2}} z \equiv z\ (mod.\ p);$$

dann liefert die Formel (4)

$$\varphi^{-1}\vartheta^{\frac{p\pm 1}{2}}\varphi z_0 \equiv z_0\ ,\ \varphi^{-1}\vartheta^{\frac{p\pm 1}{2}}\varphi z_1 \equiv z_1\ (mod.\ p),$$

oder

$$\vartheta^{\frac{p\pm 1}{2}}\varphi z_0 \equiv \varphi z_0\ ,\ \vartheta^{\frac{p\pm 1}{2}}\varphi z_1 \equiv \varphi z_1\ (mod.\ p),$$

woraus hervorgeht, dass φz_0 und φz_1 nichts Anderes als z_0 und z_1 sind. Hat man aber $\varphi z_0 \equiv z_0$ und $\varphi z_1 \equiv z_1$, so fallen die Functionen φz und $\vartheta^{\frac{p\pm 1}{2}} z$, die von der zweiten Ordnung sind, zusammen; es ist daher

$$(6).\qquad \varphi z_0 \equiv z_1\ ,\ \varphi z_1 \equiv z_0\ (mod.\ p).$$

Wenn umgekehrt diese Congruenzen (6) bestehen, so haben die Congruenzen zweiten Grades

$$\varphi^{-1}\vartheta^{\frac{p\pm1}{2}}\varphi z \equiv z\ ,\ \vartheta^{\frac{p\pm1}{2}} z \equiv z\ (mod.\ p)$$

dieselben Wurzeln, und da ihre ersten Glieder Functionen zweiter Ordnung sind, so müssen diese ersten Glieder einander gleich sein.

Zusatz I. — Es giebt $p \pm 1$ Substitutionen zweiter Ordnung φz von der Beschaffenheit, dass man

$$\varphi^{-1}\vartheta\varphi z = \vartheta^{\mu} z$$

hat, nämlich: $p+1$, wenn ϑz von der Ordnung $p+1$, $p-1$, wenn ϑz von der Ordnung $p-1$ ist.

Wenn nämlich, wie früher, z_0 und z_1 die Wurzeln der Congruenz $\vartheta z \equiv z\ (mod.\ p)$ bezeichnen, und man

$$\varphi z_0 \equiv z_1\ ,\ \varphi z_1 \equiv z_0\ (mod.\ p)$$

hat, so ist die lineare Function zweiter Ordnung φz von folgender Form:

$$\varphi z = \frac{a(z-z_0-z_1)+a' z_0 z_1}{a' z-a}.$$

Dieser Ausdruck enthält eine unbestimmte Grösse $\frac{a}{a'}$, welcher man die $p+1$ Werthe

$$0\ ,\ 1\ ,\ 2\ ,\ \ldots\ ,\ (p-1)\ ,\ \infty$$

beilegen kann. Man hat jedoch, wenn z_0 und z_1 reell sind, die beiden Werthe $\frac{a}{a'} = z_0$, $\frac{a}{a'} = z_1$ wegzulassen, für welche der Ausdruck von φz sich auf eine Constante reducirt. Die Anzahl der Substitutionen φz ist also immer gleich der Ordnung von ϑz.

Zusatz II. — Wenn ϑz eine Substitution der Ordnung $p \pm 1$ und φz eine der $p \pm 1$ Substitutionen zweiter Ordnung ist, für welche man

$$\varphi^{-1}\vartheta\varphi z = \vartheta^{\mu} z$$

hat, so erhält man ein System von $2(p \pm 1)$ conjugirten Substitutionen, dadurch dass man mit den Potenzen von ϑz die Produkte dieser Potenzen in φz verbindet. Diese $p \pm 1$ Produkte sind ausserdem eben die $p \pm 1$ Substitutionen zweiter Ordnung, welche der vorhergehenden Gleichung genügen.

Zunächst ist es klar, dass man ein conjugirtes System erhält, wenn man die beiden Systeme

$$z\,,\ \vartheta z\,,\ \vartheta^2 z\,,\ \ldots\,,\ \vartheta^{(p\pm 1)-1} z\,,$$
$$z\,,\ \varphi z\,,$$

sei es nun zur Rechten oder zur Linken, mit einander multiplicirt.

Wir wollen jetzt eins der so entstehenden Produkte

$$(1). \qquad \psi(z) = \vartheta^i \varphi z$$

näher in's Auge fassen. Da die Gleichung

$$\varphi^{-1} \vartheta \varphi z = \vartheta^{\mu} z$$

die folgende nach sich zieht:

$$\varphi^{-1} \vartheta^i \varphi z = \vartheta^{\mu i} z,$$

so hat man auch

$$(2). \qquad \psi(z) = \varphi \vartheta^{\mu i} z.$$

Die Formeln (1) und (2) liefern

$$\psi^2 z = \vartheta^i \varphi \varphi \vartheta^{\mu i} z = \vartheta^{(\mu+1) i} z,$$

und dies erfordert, dass

$$\psi^2 z = z$$

sei; denn sonst würden die Functionen ψ und φ der Gruppe der Potenzen von ϑ angehören, was mit der Voraussetzung in Widerspruch steht. Die Produkte $\vartheta^i \varphi z$ sind daher sämmtlich von der zweiten Ordnung.

Die Gleichung (1) liefert

$$\vartheta^i z = \psi \varphi z,$$

und dies lehrt, dass jede lineare Substitution $\vartheta^i z$ das Produkt zweier Substitutionen zweiter Ordnung ist.

Anmerkung. — Man erhält ein conjugirtes System der Ordnung $2n$, wenn man $p+1 = mn$ setzt und die beiden Systeme

$$z\,,\ \vartheta^m z\,,\ \vartheta^{2m} z\,,\ \ldots\,,\ \vartheta^{(n-1)m} z\,,$$
$$z\,,\ \varphi z$$

mit einander multiplicirt.

Zusatz III. — Damit zwei lineare Substitutionen, welche nicht Potenzen ein und derselben Substitution sind, gegen einander vertauschbar seien, ist erforderlich und hinreichend, dass beide von der zweiten Ordnung sind, und dass die (reellen oder imaginären) Indices, welche die eine Substitution nicht versetzt, durch die andere transponirt werden.

Es seien φ und ψ zwei lineare Substitutionen, welche nicht Potenzen ein und derselben Substitution sind. Wenn diese Substitutionen sich gegen einander vertauschen lassen, so hat (No. 470) keine von ihnen die Ordnung p; ψz ist daher eine Potenz einer Substitution ϑz der Ordnung $p+1$. Die Gleichung

$$\psi\varphi z = \varphi\psi z \text{ oder } \varphi^{-1}\psi\varphi z = \psi z$$

kann nur dann stattfinden, wenn die Gruppe der Potenzen von $\varphi^{-1}\vartheta\varphi z$ mit derjenigen der Potenzen von ϑz zusammenfällt; dies erfordert, dass φz von der zweiten Ordnung sei. In derselben Weise lässt sich darthun, dass auch ψz von der zweiten Ordnung ist. Bezeichnen dann z_0 und z_1 die Wurzeln der Congruenz $\varphi z \equiv z \ (mod.\ p)$, so sind dem vorstehenden Lehrsatze zufolge φz und ψz gegen einander vertauschbar, wenn

$$\psi z_0 \equiv z_1 \ , \ \psi z_1 \equiv z_0 \ (mod.\ p)$$

ist. Es liegt auf der Hand, dass die eine dieser Bedingungen die andere nach sich zieht.

472. Lehrsatz IV. — Es seien ϑz eine lineare Substitution $(p+1)^{\text{ter}}$ Ordnung für den Modul p und ωz eine beliebige lineare Substitution. Dann kann man der Gleichung

$$\vartheta^m \omega \vartheta^n z = Ez,$$

in welcher Ez eine lineare und ganze Substitution bezeichnet, dadurch genügen, dass man einer der Zahlen m und n, gleichgiltig welcher, irgend einen der Werthe $0, 1, 2, 3, \ldots, p$ beilegt; der Werth der andern Zahl ist sodann bestimmt.

Da die Substitution ϑz von der Ordnung $p+1$ ist, so nehmen die Potenzen

$$z \ , \ \vartheta z \ , \ \vartheta^2 z \ , \ \ldots \ , \ \vartheta^p z$$

in einer gewissen Reihenfolge die Werthe

$$0 \ , 1 \ , 2 \ , 3 \ , \ldots , (p-1) \ , \infty$$

an, welchen Werth man auch z beilegen mag. Wir setzen nun

$$\vartheta^n \infty = z_0 \ , \ \omega z_0 = z_1 \ , \ \vartheta^m z_1 = \infty .$$

Wenn die Zahl n gegeben ist, so bestimmt die erste dieser Formeln z_0, die zweite liefert darauf z_1, und sodann ist m durch die dritte Formel bestimmt. Ist dagegen die Zahl m gegeben, so

bestimmt die dritte Formel z_1; dann erhält man $z_0 = \omega^{-1} z_1$ aus der zweiten und endlich n aus der ersten Formel. Man hat danach

$$\vartheta^m \omega \vartheta^n \infty = \infty,$$

d. h. die lineare Function $\vartheta^m \omega \vartheta^n z$ wird für $z = \infty$ unendlich gross; sie ist mithin eine ganze Function.

Zusatz. — Wir nehmen an, die Determinante der Substitution ωz sei quadratischer Rest des Moduls p und r bezeichne eine primitive Wurzel für diesen Modul; ausserdem wählen wir die ganzen Zalen m, n so, dass

$$\vartheta^{p+1-m} \omega \vartheta^n z$$

eine ganze Substitution sei, und setzen

$$f_{2\mu} z = \vartheta^{2\mu} z \;,\; f_{2\mu+1} z = \vartheta^{2\mu+1}(rz);$$

dann ist

$$f_m^{-1} \omega f_n z$$

eine ganze Substitution, deren Determinante quadratischer Rest von p ist.

Jenachdem nämlich m und n gerade oder ungerade sind, hat die in Rede stehende Substitution eine der Formen

$$\vartheta^{-m} \omega \vartheta^n z \;,\; \vartheta^{-m} \omega \vartheta^n rz \;,\; \frac{1}{r} \vartheta^{-m} \omega \vartheta^n z \;,\; \frac{1}{r} \vartheta^{-m} \omega \vartheta^n rz;$$

sie ist daher eine ganze Substitution. Da sie zudem das Produkt von drei Substitutionen $f_m^{-1} z$, ωz, $f_n z$ ist, deren Determinanten quadratische Reste von p sind, so ist auch ihre Determinante quadratischer Rest von p.

Beispiel. Wir setzen $p = 7$, $r = 3$ voraus und nehmen

$$\vartheta z = \frac{z+6}{z+4} \;,\; \omega z = \frac{z+2}{z+6};$$

dann ergiebt sich

$$\begin{aligned}
\tfrac{1}{3} \vartheta^7 \omega \vartheta^0 z &= z, & \vartheta^2 \omega \vartheta^4 z &= 4z + 4, \\
\vartheta^0 \omega \vartheta 3z &= z, & \tfrac{1}{3} \vartheta \omega \vartheta^5 3z &= 2z + 6, \\
\tfrac{1}{3} \vartheta^5 \omega \vartheta^2 z &= 4z + 4, & \vartheta^4 \omega \vartheta^6 z &= z + 3, \\
\vartheta^6 \omega \vartheta^3 3z &= 2z + 6 \;, & \tfrac{1}{3} \vartheta^3 \omega \vartheta^7 3z &= 4z + 4.
\end{aligned}$$

Ueber die Substitutionen von fünf und von sieben Buchstaben.

473. Wenn die Primzahl p gleich 3 ist, so sind die Substitutionen der $p-1$ Indices z

$$0\,,1\,,2\,,3\,,\ldots,(p-1)$$

sämmtlich linear und ganz.

Den analytischen Ausdruck der Substitutionen für den Fall von fünf Buchstaben hat Betti gegeben; dieselbe Aufgabe hinsichtlich der Substitutionen von sieben Buchstaben ist später von Hermite gelöst worden. Diese wichtigen Resultate wollen wir hier darlegen.

Substitutionen von fünf Buchstaben. — Wir betrachten zunächst den Fall von 5 Indices. Nach Nr. 465 sind die reducirten Formen der Substitutionen

$$\vartheta z \equiv z\;,\;z^2\;,\;z^3+az\;(mod.\;5).$$

Die zweite dieser Formen ist auszuschliessen, da aus ihr

$$[\vartheta z]^2 \equiv z^4 \equiv 1\;(mod.\;5)$$

hervorgeht. Die dritte Form liefert

$$[\vartheta z]^2 \equiv z^6+2az^4+a^2z^2 \equiv (1+a^2)z^2+2a,$$

und um den von z unabhängigen Term zum Wegfall zu bringen, hat man $a=0$ zu setzen. Da ferner alle übrigen Bedingungen (Nr. 465) durch den Ausdruck $\vartheta z \equiv z^3$ erfüllt werden, so sieht man, dass alle Substitutionen für ein System von fünf Indices in den beiden Formen

$$\alpha z+\beta\;,\;\alpha(z+\beta)^3+\gamma$$

enthalten sind, in welchen nur der Werth $\alpha=0$ nicht genommen werden darf.

474. Substitutionen von sieben Buchstaben. — Im Falle von sieben Indices können die reducirten Formen nur folgende sein:

$$\vartheta z \equiv z\,,\,z^2,\,z^3+az\;,\;z^4+az^2+bz\;,\;z^5+az^3+bz^2+cz.$$

Es sind nun zunächst die zweite und die dritte dieser Formen fortzulassen, weil im Kubus der zweiten und im Quadrate der dritten der von z unabhängige Term stehen bleibt.

Ist

$$\vartheta z \equiv z^4+az^2+bz,$$

so sieht man sofort, dass der unabhängige Term in $[\vartheta z]^2$ a ist; man hat daher $a \equiv 0$. Weiter ergiebt sich

$$\left.\begin{aligned}(z^4 + bz)^3 &= z^{12} + 3bz^9 + 3b^2z^6 + b^3z^3 \\ &\equiv (b^3 + 3b)\,z^3 + (3b^2 + 1)\end{aligned}\right\} (mod.\ 7),$$

und dies erfordert, dass man

$$3b^2 + 1 \equiv 0\ ,\ b \equiv \pm 3\ (mod.\ 7)$$

mache. Man hat also die beiden Formen

$$\vartheta z = z^4 + 3z\ ,\ \vartheta z = z^4 - 3z;$$

die zweite derselben lässt sich aber durch die in Nr. 465 angegebene Transformation auf die erste zurückführen; denn macht man

$$\Theta z = a^2\vartheta(az) = a^2(a^4z^4 + 3az) = z^4 + 3a^3z,$$

so reducirt sich Θz auf

$$\Theta z = z^4 - 3z,$$

wenn man

$$a^3 \equiv -1\ (mod.\ 7)$$

voraussetzt, d. h. wenn man a als quadratischen Nichtrest von 7 annimmt. Man erhält jetzt die folgende Reihe der Potenzen von ϑz:

$$\left.\begin{aligned}\vartheta z &\equiv z^4 + 3z, \\ [\vartheta z]^2 &\equiv 6z^5 + 3z^2, \\ [\vartheta z]^3 &\equiv z^3, \\ [\vartheta z]^4 &\equiv 3z^4 + z, \\ [\vartheta z]^5 &\equiv 3z^5 + 6z^2\end{aligned}\right\} (mod.\ 7),$$

so dass alle übrigen Bedingungen von selbst erfüllt sind.

Ist endlich

$$\vartheta z \equiv z^5 + az^3 + bz^2 + cz\ (mod.\ 7),$$

so erhält man, wenn der im Quadrat, im Kubus und in der vierten Potenz von ϑz vorkommende von z unabhängige Term gleich Null gesetzt wird,

$$2c + a^2 \equiv 0,$$
$$b(3 + 6ac + b^2) \equiv 0,$$
$$ab^2 + 4b^2c^2 + 2(2a + c^2)(1 + 2ac + b^2) \equiv 0.$$

Die zweite Bedingung wird erfüllt, wenn man

$$b \equiv 0$$

setzt, wodurch die dritte sich auf

$$(2a + c^2)\ (1 + 2ac) \equiv 0$$

reducirt. Ersetzt man hierin c durch den Werth $-\frac{1}{2}a^2 \equiv 3a^2$, welcher sich aus der ersten Congruenz ergiebt, so erhält man die Identität

$$2(a + a^4)\ (1 - a^3) \equiv 2(a - a^7) \equiv 0.$$

Man hat also den folgenden Ausdruck

$$\vartheta z \equiv z^5 + az^3 + 3a^2 z,$$

in welchem a unbestimmt bleibt, den man aber auf den Fall $a \equiv 0$ und mittels der Relation

$$\alpha \vartheta(\alpha z) = z^5 + a\alpha^4 z^3 + 3a^2\alpha^2 z$$

auf die Fälle $a \equiv 1$, $a \equiv 3$ zurückführen kann. Es lässt sich leicht zeigen, dass die 5te Potenz unseres Ausdrucks von ϑz keinen von z unabhängigen Term enthält, so dass die letzte Bedingung von selbst erfüllt ist.

Nehmen wir jetzt an, b sei nach dem Modul 7 von Null verschieden. Die erste der oben angegebenen Bedingungen liefert

$$c \equiv 3a^2,$$

und durch Einsetzung dieses Werthes gehen die beiden anderen Bedingungen über in

$$3 - 3a^3 + b^2 \equiv 0,$$
$$a + a^4 \equiv 0.$$

Man erhält daraus die beiden Lösungen

$$a \equiv 0\ ,\ \ b \equiv \pm 2$$

und

$$a^3 \equiv -1\ ,\ \ b \equiv \pm 1,$$

und es ergeben sich somit die neuen reducirten Formen:

$$\vartheta z \equiv z^5 \pm 2z^2,$$
$$\vartheta z \equiv z^5 + az^3 \pm z^2 + 3a^2 z;$$

hier ist a quadratischer Nichtrest von 7. Durch die oben schon angewandte Transformation lassen sich diese beiden Formen auf die folgenden zurückführen:

$$\vartheta z = z^5 + 2z^2,$$
$$\vartheta z = z^5 + 3z^3 \pm z^2 - z.$$

Fassen wir die Ergebnisse unserer Betrachtung zusammen, so sehen wir, dass die

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 5040$$

Substitutionen der Indices

$$0, 1, 2, 3, 4, 5, 6$$

sämmtlich durch

$$\alpha z + \beta\ ,\ \alpha\vartheta(z+\beta)+\gamma$$

dargestellt werden können, wenn die Function ϑz der Reihe nach folgende Formen annimmt:

$$z^4 \pm 3z,$$
$$z^5 \pm 2z^2,$$
$$z^5 + az^3 + 3a^2 z \text{ (a ist unbestimmt)},$$
$$z^5 + az^3 \pm z^2 + 3a^2 z \text{ (a ist Nichtrest von 7)}.$$

475. Hermite hat die vorstehenden Resultate zuerst in den Annalen von Tortolini veröffentlicht und sie später durch Bemerkungen vervollständigt, die wir nicht übergehen können.

Wir betrachten die beiden reducirten Formen z^4+3z, z^5+2z^2, welche unter den oben erhaltenen sich vorfinden, und vertheilen die Werthe von z in zwei Gruppen, von denen die eine die quadratischen Reste, die zweite die quadratischen Nichtreste von 7 enthält. Man findet

$$z^4 + 3z \equiv 4z \text{ (z ist Rest von 7)},$$
$$\equiv 2z \text{ (z ist Nichtrest von 7)},$$

und

$$z^5 + 2z^2 \equiv 3z^2 \text{ (z ist Rest von 7)},$$
$$\equiv z^2 \text{ (z ist Nichtrest von 7)}.$$

Zweitens betrachten wir die reducirte Form z^5+z^3+3z und theilen die Indices in kubische Reste und Nichtreste von 7 ein; dann ergiebt sich

$$z^5 + z^3 + 3z \equiv -2z \text{ (z ist kubischer Rest von 7)},$$
$$\equiv +2z \text{ (z ist kubischer Nichtrest von 7)}.$$

Endlich wollen wir die beiden Substitutionen z^5+3z^3-z und $z^5+3z^3 \pm z^2 - z$ betrachten. Auch diese lassen sich auf die Form von Mononomen bringen, aber auf eine ganz andere Weise. Man hat nämlich

$$z^5 + 3z^3 - z \equiv 3z^2 (z < \tfrac{7}{2}),$$
$$\equiv -3z^2\ (z > \tfrac{7}{2}),$$

und daraus folgt, wenn man $\varepsilon = \pm 1$ macht,

$$z^5 + 3z^3 + \varepsilon z^2 - z \equiv (3+\varepsilon)z^2\ (z < \tfrac{7}{2}),$$
$$\equiv (-3+\varepsilon)z^2\ (z > \tfrac{7}{2}).$$

Diese Resultate, sagt Hermite, berechtigen uns bis zu einem gewissen Punkte zu der Voraussetzung, dass die Ausdrücke, welche man in der Untersuchung der analytischen Formen der Substitutionen von Buchstaben, deren Anzahl p eine Primzahl ist, reducirte genannt hat, sich auf viel einfachere zurückführen lassen, wenn man die Werthe des Index als Potenzreste oder Nichtreste ansieht, deren Exponent in $p-1$ aufgeht, oder auch, wenn man sich diese Werthe in zwei Reihen getheilt denkt, von denen die eine aus Zahlen besteht, die kleiner als $\frac{p}{2}$ sind, die zweite aus Zahlen, die grösser als $\frac{p}{2}$ sind.

476. Hat man z. B. für eine beliebige Primzahl p eine reducirte Substitution von der Form

$$\vartheta z = a z^{\omega}(z^{\frac{p-1}{2}}+1) - b z^{\omega}(z^{\frac{p-1}{2}}-1),$$

so kann man offenbar einfacher schreiben

$$\vartheta z = 2 a z^{\omega} \text{ (wenn } z \text{ Rest von } p \text{ ist)},$$
$$\vartheta z = 2 b z^{\omega} \text{ (wenn } z \text{ Nichtrest von } p \text{ ist)}.$$

In diese Kategorie von Substitutionen gehört im Falle $p=7$ die reducirte Substitution

$$\vartheta z = - z^5 - 2 z^2,$$

die so beschaffen ist, dass man

$$\vartheta[\vartheta z] \equiv z$$

und

$$\vartheta[a\vartheta(z)+b] = 2 a b^4 \vartheta(z+\frac{2}{a^4 b}) + \frac{1-a}{a}(b^5+2b^2)$$

hat, vorausgesetzt dass a quadratischer Rest von 7 ist.

Daraus geht hervor, dass die Substitutionen, welche die Ausdrücke

$$az+b\ ,\ a\vartheta(z+b)+c$$

darstellen, ein conjugirtes System bilden, wenn a Rest von 7 ist. Der erste Ausdruck liefert 3×7 oder 21, der zweite 3×7^2 oder 147 Substitutionen. Es giebt also ein System von 168 conjugirten Substitutionen von sieben Buchstaben; der Index dieses Systems ist gleich 80. Dieses wichtige Resultat ist zuerst von Kronecker constatirt worden.

Fünftes Kapitel.

Anwendungen der Theorie der Substitutionen.

Ueber die verschiedenen Werthe, welche eine Function mehrerer Veränderlichen durch die Substitutionen dieser Veränderlichen annimmt.

477. Die in den vorhergehenden Kapiteln dargelegten Principien wollen wir jetzt auf die Functionen mehrerer Veränderlichen anwenden; namentlich wollen wir unser Augenmerk auf die verschiedenen Werthe richten, welche diese Functionen in Folge der Substitutionen der Veränderlichen annehmen. Für unsere Zwecke genügt es zwar, die rationalen und sogar nur die ganzen Functionen zu betrachten; indess beziehen sich die nachstehenden Entwicklungen auf alle völlig bestimmten Functionen.

Wir bezeichnen mit V eine völlig bestimmte Function der n Veränderlichen

$$x_0 \,,\, x_1 \,,\, x_2 \,,\, \ldots \,,\, x_{n-1} \,,$$

bilden die $N = 1.2.3 \ldots n$ Substitutionen dieser Veränderlichen und vollziehen alle diese Substitutionen der Reihe nach in V; auf diese Weise erhalten wir N Resultate

$$V \,,\, V^{(1)} \,,\, V^{(2)} \,,\, \ldots \,,\, V^{(N-1)}. \tag{1}$$

Wenn die Function V symmetrisch ist, so sind die N Resultate (1) sämmtlich einander gleich; sie sind dagegen sämmtlich von einander verschieden, wenn die Function V gar keine Symmetrie besitzt. Dieser Fall tritt im Besonderen ein, wenn man

$$V = \alpha_0\, x_0 + \alpha_1\, x_1 + \alpha_2\, x_2 \ldots + \alpha_{n-1}\, x_{n-1}$$

hat, wo $\alpha_0 \,,\, \alpha_1 \,,\, \ldots \,,\, \alpha_{n-1}$ ungleiche Coefficienten sind.

Bezeichnet allgemein μ die Anzahl derjenigen der Functio-

nen (1), welche gleich V sind, so ist μ auch gleich der Anzahl der Substitutionen, die man in V ausführen kann, ohne diese Function zu ändern. Diese μ Substitutionen seien

(2). $$1\,,\ S_1\,,\ S_2\,,\ \ldots\,,\ S_{\mu-1}.$$

Da die Function V keine Aenderung erleidet, wenn man zwei oder mehrere der Substitutionen (2) in irgend einer Reihenfolge vollzieht, so machen diese Substitutionen offenbar ein conjugirtes System aus.

In No. 413 haben wir gesehen, dass die N Substitutionen der n Veränderlichen durch

(3). $$\left\{\begin{array}{llllll} 1 & , S_1 & , S_2 & , \ldots & , S_{\mu-1} & , \\ T_1 & , T_1\,S_1 & , T_1\,S_2 & , \ldots & , T_1\,S_{\mu-1} & , \\ T_2 & , T_2\,S_1 & , T_2\,S_2 & , \ldots & , T_2\,S_{\mu-1} & , \\ \cdot & \cdot & \cdot & \cdot & \cdot & , \\ T_{\nu-1} & , T_{\nu-1}\,S_1 & , T_{\nu-1}S_2 & , \ldots & , T_{\nu-1}\,S_{\mu-1} & \end{array}\right.$$

dargestellt werden können; mithin lassen sich die $N = \mu\nu$ Functionen (1) durch

(4). $$\left\{\begin{array}{llllll} V_0 & , V_0^{(1)} & , V_0^{(2)} & , \ldots & , V_0^{(\mu-1)} & , \\ V_1 & , V_1^{(1)} & , V_1^{(2)} & , \ldots & , V_1^{(\mu-1)} & , \\ V_2 & , V_2^{(1)} & , V_2^{(2)} & , \ldots & , V_2^{(\mu-1)} & , \\ \cdot & \cdot & \cdot & \cdot & \cdot & , \\ V_{\nu-1} & , V_{\nu-1}^{(1)} & , V_{\nu-1}^{(2)} & , \ldots & , V_{\nu-1}^{(\mu-1)} & \end{array}\right.$$

darstellen, wo allgemein $V_i^{(j)}$ das Resultat bezeichnet, welches man erhält, wenn man in V zuerst die Substitution S_j und darauf die Substitution T_i ausführt. Im Falle $j = 0$ ist die Substitution S_j auf die Einheit zu reduciren; wir schreiben dann V_i statt $V_i^{(0)}$.

Da die Substitutionen S die Function V oder V_0 nicht ändern, so sieht man, dass die Terme ein und derselben Horizontalreihe der Tabelle (4) einander gleich, und dass die verschiedenen Werthe von V nur folgende sind:

(5). $$V_0\,,\ V_1\,,\ V_2\,,\ \ldots\,,\ V_{\nu-1}.$$

478. Wenn eine Function durch eine Substitution keine Aenderung erleidet, so werden wir der Kürze wegen sagen, die

Function lasse diese Substitution zu. Man kann dann folgenden Satz aussprechen:

Lehrsatz I. — Die Substitutionen einer Function mehrerer Veränderlichen bilden ein conjugirtes System, und der Index dieses Systems ist gleich der Anzahl der verschiedenen Werthe, welche die Function in Folge der Substitutionen annehmen kann.

Dieser Lehrsatz gestattet mehrere Folgerungen (No. 414 und No. 432), von denen wir folgende hervorheben müssen:

Zusatz I. — Die Anzahl der verschiedenen Werthe einer Function von n Veränderlichen ist ein Divisor des Produkts $1 . 2 . 3 \ldots n$.

Zusatz II. — Die Anzahl der verschiedenen Werthe einer Function von n Veränderlichen kann nicht unter n hinabsinken, ohne sich auf 1 oder auf 2 zu reduciren; nur der Fall $n = 4$ macht eine Ausnahme.

Zusatz III. — Eine Function von n Veränderlichen, welche genau n verschiedene Werthe hat, ist in Beziehung auf $n - 1$ Veränderliche symmetrisch; nur der Fall $n = 6$ macht eine Ausnahme.

Es ist zu beachten, dass wenn man irgend eine Substitution an den ν Functionen (5) vollzieht, diese Functionen sich nur gegeneinander vertauschen können. Bezeichnet also V eine unbestimmte Grösse, so ist das Produkt

$$(V - V_0)\ (V - V_1)\ \ldots\ (V - V_{\nu-1})$$

eine symmetrische Function. Daraus folgt, dass jede symmetrische Function der Functionen (5) symmetrisch in Beziehung auf die Veränderlichen x ist. Wir hatten bereits in No. 180 Gelegenheit, diese Bemerkung zu machen.

479. Der eben hergeleitete Satz lässt sich in folgender Weise umkehren:

Lehrsatz II. — Es giebt immer Functionen, welche die Substitutionen eines gegebenen conjugirten Systems und keine andere Substitution zulassen.

Es seien

$$(1). \qquad 1\ ,\ S_1\ ,\ S_2\ ,\ \ldots\ ,\ S_{\mu-1}$$

die gegebenen conjugirten Substitutionen, und es werde mit X eine Function der n Veränderlichen

$$x_0\,,\,x_1\,,\,x_2\,,\,\ldots\,,\,x_{n-1}$$

bezeichnet, deren N Werthe sämmtlich von einander verschieden sind; man kann z. B.

$$X = \alpha_0\,x_0 + \alpha_1\,x_1 + \alpha_2\,x_2 + \cdots + \alpha_{n-1}\,x_{n-1}$$

nehmen, wo $\alpha_0\,,\,\alpha_1\,,\,\ldots\,,\,\alpha_{n-1}$ ungleiche Zahlen sind.

Stellen nun

$$X_0\,,\,X_1\,,\,X_2\,,\,\ldots\,,\,X_{\mu-1}$$

die Resultate dar, welche man erhält, wenn man an X die μ Substitutionen (1) vollzieht, und wird

$$V = X_0\,X_1\,X_2\,\ldots\,X_{\mu-1}$$

gesetzt, so lässt die Function V offenbar die μ Substitutionen (1) und keine andere Substitution zu.

Anmerkung. — Setzt man

$$V = f\,(X_0\,,\,X_1\,,\,X_2\,,\,\ldots\,,\,X_{\mu-1})\,,$$

wo f eine symmetrische Function von $X_0\,,\,X_1\,,\,\ldots\,,\,X_{\mu-1}$ bezeichnet, so lässt die Function V die Substitutionen (1) zu; sie kann aber noch andere Substitutionen zulassen, wenn die Function f eine passende Form hat. Macht man z. B.

$$V = X_0 + X_1 + \cdots + X_{\mu-1}\,,$$

so ist V eine symmetrische Function der Veränderlichen

$$x_0\,,\,x_1\,,\,\ldots\,,\,x_{n-1}.$$

Aehnliche Functionen.

480. Zwei Functionen von n Veränderlichen werden **ähnlich** genannt, wenn sie dieselben Substitutionen zulassen.

So sind die Functionen

$$x_0\,x_1 + x_2\,x_3 \quad , \quad (x_0 + x_1)\,(x_2 + x_3)$$

der vier Veränderlichen $x_0\,,\,x_1\,,\,x_2\,,\,x_3$ ähnlich, denn beide lassen die acht Substitutionen

$$\begin{array}{l|l|l|l|}
1 & (x_0\,,\,x_1) & (x_0\,,\,x_2)\;(x_1\,,\,x_3) & (x_0\,,\,x_2\,,\,x_1\,,\,x_3) \\
 & (x_2\,,\,x_3) & (x_0\,,\,x_3)\;(x_1\,,\,x_2) & (x_0\,,\,x_1)\;(x_2\,,\,x_3) \\
 & & & (x_0\,,\,x_3\,,\,x_1\,,\,x_2)
\end{array}$$

zu, welche ein conjugirtes System mit dem Index 3 bilden.

Lagrange hat eine wichtige Eigenschaft der ähnlichen Functionen entdeckt, die sich folgendermassen aussprechen lässt:

Wenn zwei ähnliche Functionen der n Veränderlichen $x_0, x_1, x_2, \ldots, x_{n-1}$ gegeben sind, so lässt sich jede dieser Functionen rational durch die andere ausdrücken, und die Coefficienten dieses Ausdrucks sind symmetrische Functionen der n Veränderlichen.

Dieser Satz ist in einem weit allgemeineren enthalten, den wir jetzt herleiten wollen:

Lehrsatz. — Es seien zwei Functionen der n Veränderlichen $x_0, x_1, x_2, \ldots, x_{n-1}$, nämlich

$$V = F(x_0, x_1, x_2, \ldots, x_{n-1}),$$

$$y = f(x_0, x_1, x_2, \ldots, x_{n-1})$$

gegeben; wenn die Function y alle Substitutionen von V zulässt, so ist sie durch eine rationale Function von V ausdrückbar, in welcher die Coefficienten symmetrische Functionen sind.

Es seien nämlich

$$1, S_1, S_2, \ldots, S_{\mu-1}$$

die conjugirten Substitutionen von V und

$$1, T_1, T_2, \ldots, T_{\nu-1}$$

die ν Substitutionen, mittels welcher man aus V die ν verschiedenen Werthe herleitet, welche diese Function annehmen kann. Endlich setzen wir noch voraus, V_ϱ und y_ϱ seien die Resultate, die man erhält, wenn man die Substitution T_ϱ an V und an y vollzieht. Wir nehmen $T_0 = 1$ an, so dass V_0 und y_0 nichts Anderes als V und y bedeuten.

Macht man

$$\psi(V) = (V - V_0)(V - V_1)(V - V_2)\ldots(V - V_{\nu-1}),$$

so erhält man durch Entwicklung des zweiten Gliedes

$$\psi(V) = V^\nu + P_1 V^{\nu-1} + P_2 V^{\nu-2} + \cdots + P_{\nu-1} V + P_\nu,$$

wo $P_1, P_2, \ldots, P_\nu$ symmetrische Functionen sind. Hier wird V als eine unbestimmte Grösse angesehen, und die Gleichung

$$\psi(V) = 0 \tag{1}$$

hat die Wurzeln

$$V_0, V_1, V_2, \ldots, V_{\nu-1}. \tag{2}$$

Betrachten wir jetzt die Function

$$V^m y,$$

in welcher m irgend eine ganze Zahl ist. Der Voraussetzung nach lässt diese Function alle Substitutionen von V zu. Wenn sie eine noch grössere Anzahl von Substitutionen zulässt, so können dieselben durch

$$\begin{array}{lllll} 1 & , S_1 & , S_2 & , \dots, & S_{\mu-1}, \\ R_1 & , R_1 S_1 & , R_1 S_2 & , \dots, & R_1 S_{\mu-1}, \\ \dots & \dots & \dots & \dots & \dots, \\ R_{\varrho-1} & , R_{\varrho-1} S_1 & , R_{\varrho-1} S_2 & , \dots, & R_{\varrho-1} S_{\mu-1} \end{array}$$

dargestellt werden, und durch Multiplication mit gewissen Substitutionen

$$1 \, , \, Q_1 \, , \, Q_2 \, , \, \dots \, , \, Q_{\lambda-1}$$

erhält man (No. 413) hieraus alle $1.2.3\dots n$ Substitutionen der n Veränderlichen. Daraus geht hervor, dass die Substitutionen T die Produkte der Substitutionen

$$1 \, , \, R_1 \, , \, R_2 \, , \, \dots , \, R_{\varrho-1} \, ,$$

welche $V^m y$ unverändert lassen, in die Substitutionen

$$1 \, , \, Q_1 \, , \, Q_2 \, , \, \dots \, , \, Q_{\lambda-1}$$

sind. Wendet man daher auf die Function $V^m y$ die ν Substitutionen T an, so erhält man die λ verschiedenen Werthe dieser Function, jeden ϱ mal wiederholt; folglich ist die Summe

$$V_0^m y_0 + V_1^m y_1 + V_2^m y_2 + \dots + V_{\nu-1}^m y_{\nu-1}$$

eine symmetrische Function der n Veränderlichen $x_0, x_1, \dots, x_{n-1}$. Ertheilt man also m der Reihe nach die Werthe $0, 1, 2, \dots, (\nu-1)$ und setzt

$$(3). \quad \left\{ \begin{array}{l} y_0 + y_1 + y_2 + \dots + y_{\nu-1} = t_0 \quad , \\ V_0 \; y_0 + V_1 \, y_1 \; + \dots + V_{\nu-1} y_{\nu-1} = t_1 \quad , \\ V_0^2 \; y_0 + V_1^2 \, y_1 \; + \dots + V_{\nu-1}^2 y_{\nu-1} = t_2 \quad , \\ \dots \dots \dots \dots \dots \dots \dots \dots , \\ V_0^{\nu-1} y_0 + V_1^{\nu-1} y_1 + \dots + V_{\nu-1}^{\nu-1} y_{\nu-1} = t_{\nu-1} \, , \end{array} \right.$$

so werden $t_0 \, , \, t_1 \, , \, \dots$ symmetrische Functionen sein.

Wir addiren die Gleichungen (3), nachdem wir sie beziehungsweise mit den unbestimmten Factoren

$$\lambda_0 \, , \, \lambda_1 \, , \, \lambda_2 \, , \, \dots \, , \, \lambda_{\nu-2} \, , \, 1$$

multiplicirt haben, und machen der Kürze wegen

$$(4). \qquad \varphi(V) = V^{\nu-1} + \lambda_{\nu-2} V^{\nu-2} + \cdots + \lambda_1 V + \lambda_0;$$

es ergiebt sich

$$(5), \qquad \begin{cases} y_0 \varphi(V_0) + y_1 \varphi(V_1) + \cdots + y_{\nu-1} \varphi(V_{\nu-1}) \\ = t_0 \lambda_0 + t_1 \lambda_1 + \cdots + t_{\nu-2} \lambda_{\nu-2} + t_{\nu-1}. \end{cases}$$

Will man nun z. B. den Werth von y_ϱ ermitteln, so genügt es, die Factoren $\lambda_0, \lambda_1, \ldots$ in der Weise zu bestimmen, dass

$$(6). \quad \begin{cases} \varphi(V_0) = 0, \varphi(V_1) = 0, \ldots, \varphi(V_{\varrho-1}) = 0, \\ \qquad \varphi(V_{\varrho+1}) = 0, \ldots, \varphi(V_{\nu-1}) = 0 \end{cases}$$

ist; dann liefert die Gleichung (5)

$$(7). \qquad y_\varrho = \frac{t_0 \lambda_0 + t_1 \lambda_1 + \cdots + t_{\nu-2} \lambda_{\nu-2} + t_{\nu-1}}{\varphi(V_\varrho)},$$

und man hat nur noch die Werthe von $\lambda_0, \lambda_1, \ldots$ zu ermitteln, was sehr leicht auf folgende Weise geschieht:

Die Gleichungen (6), welche diese Factoren bestimmen, drücken aus, dass die Gleichung

$$\varphi(V) = 0$$

die Wurzeln $V_0, V_1, \ldots, V_{\varrho-1}, V_{\varrho+1}, \ldots, V_{\nu-1}$ hat. Nun hat aber die Gleichung (1)

$$\psi(V) = 0$$

eben dieselben Wurzeln und ausserdem noch die Wurzel V_ϱ; ferner hat die höchste Potenz von V in jeder der Functionen $\varphi(V)$, $\psi(V)$ den Coefficienten Eins; es besteht somit die Identität

$$\varphi(V) = \frac{\psi(V)}{V - V_\varrho},$$

oder, wenn das zweite Glied entwickelt wird,

$$\varphi(V) = \begin{array}{r|r|r} V^{\nu-1} + P_1 & V^{\nu-2} + P_2 & V^{\nu-3} + \cdots + P_{\nu-1} \\ + V_\varrho & + P_1 V_\varrho & + P_{\nu-2} V_\varrho \\ & + V_\varrho^2 & + P_{\nu-3} V_\varrho^2 \\ & & \cdots\cdots \\ & & + P_1 V_\varrho^{\nu-2} \\ & & + V_\varrho^{\nu-1}. \end{array}$$

Durch Vergleichung dieses Werthes von $\varphi(V)$ mit dem in (4) angegebenen erhält man folgende Werthe der Factoren λ:

$$(8). \quad \begin{cases} \lambda_{\nu-2} = P_1 + V_\varrho \,, \\ \lambda_{\nu-3} = P_2 + P_1 V_\varrho + V_\varrho^2 \,, \\ \lambda_{\nu-4} = P_3 + P_2 V_\varrho + P_1 V_\varrho^2 + V_\varrho^3 \,, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \lambda_0 = P_{\nu-1} + P_{\nu-2} V_\varrho + \cdots + P_1 V_\varrho^{\nu-2} + V_\varrho^{\nu-1} \,. \end{cases}$$

Da diese Factoren sämmtlich aus V_ϱ und den symmetrischen Functionen P gebildet sind, so ist dasselbe mit y_ϱ der Fall. Man kann dem Ausdruck von y_ϱ eine sehr einfache Form geben. Macht man der Kürze wegen

$$\begin{aligned} s_{\nu-1} &= t_{\nu-1} + P_1 t_{\nu-2} + P_2 t_{\nu-3} + \cdots + P_{\nu-2} t_1 + P_{\nu-1} t_0 \,, \\ s_{\nu-2} &= t_{\nu-2} + P_1 t_{\nu-3} + P_2 t_{\nu-4} + \cdots + P_{\nu-2} t_0 \,, \\ s_{\nu-3} &= t_{\nu-3} + P_1 t_{\nu-4} + \cdots + P_{\nu-3} t_0 \,, \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \,, \\ s_1 &= t_1 + P_1 t_0 \,, \\ s_0 &= t_0 \,, \end{aligned}$$

und bezeichnet den Zähler des durch Gleichung (7) gegebenen Werthes von y_ϱ mit $\Theta(V_\varrho)$, so ist

$$(9). \quad \Theta(V_\varrho) = s_0 V_\varrho^{\nu-1} + s_1 V_\varrho^{\nu-2} + \cdots + s_{\nu-2} V_\varrho + s_{\nu-1} \,.$$

Der Nenner des Ausdrucks von y_ϱ ist gleich $\varphi(V_\varrho)$, d. h. gleich dem Werthe, welchen die Function

$$\frac{\psi(V)}{V - V_\varrho}$$

für $V = V_\varrho$ annimmt; dieser Werth ist

$$(10). \quad \psi'(V_\varrho) = \nu V_\varrho^{\nu-1} + (\nu - 1) P_1 V_\varrho^{\nu-2} + \cdots + P_{\nu-1} \,,$$

wenn ψ' die Abgeleitete von ψ bezeichnet. Man hat daher

$$(11). \qquad y_\varrho = \frac{\Theta(V_\varrho)}{\psi'(V_\varrho)} \,,$$

oder

$$(12). \qquad y = \frac{\Theta(V)}{\psi'(V)} \,;$$

in dieser letzten Formel wird unter V irgend einer der Werthe $V_0, V_1, \ldots,$ und unter y der entsprechende Term der Reihe $y_0, y_1, \ldots,$ verstanden.

Die Formel (12) beweist den vorliegenden Lehrsatz, indem sie y als rationale Function von V darstellt. Wir fügen hinzu,

dass die in No. 182 dargelegte Methode es gestattet, den Ausdruck (12) auf die einfachere Form

$$y = \Pi(V)$$

zu bringen, wo Π eine ganze Function bezeichnet, deren Grad in V höchstens $\nu - 1$ ist, und in welcher die Coefficienten von V symmetrische Functionen der Veränderlichen x sind.

Ueber die Bildung der Functionen von n Veränderlichen, welche gegebene Substitutionen zulassen.

481. Die Aufgabe, die Functionen von n Veränderlichen zu bilden, welche eine gegebene Anzahl ν verschiedener Werthe haben, wird durch die vorhergehenden Lehrsätze auf die Bestimmung der Systeme conjugirter Substitutionen zurückgeführt, deren Index gleich ν ist. Kennt man nämlich ein solches System, so erhält man mit Hilfe des Lehrsatzes der No. 479 leicht eine entsprechende Function V, welche genau ν verschiedene Werthe hat, und die übrigen ähnlichen Functionen lassen sich, wie wir uns eben überzeugt haben, als ganze Functionen $(\nu - 1)^{\text{ten}}$ Grades von V ausdrücken, in denen die Coefficienten der Potenzen von V symmetrische Functionen sind.

Betrachten wir z. B. die Functionen, welche zwei verschiedene Werthe haben. Die Substitutionen dieser Functionen bilden ein conjugirtes System, dessen Index gleich 2 ist. Dieses System ist einzig in seiner Art, wie in No. 417 gezeigt wurde, und es besteht aus den Substitutionen, welche einer geraden Anzahl von Transpositionen äquivalent sind. Die in Rede stehenden Functionen V sind daher ähnlich, und wenn eine derselben mit P bezeichnet wird, so ist der allgemeine Ausdruck von V

$$V = A + BP,$$

wo A und B symmetrische Functionen sind. Man kann für P die alternirende Function der n Veränderlichen $x_0, x_1, \ldots, x_{n-1}$ nehmen, die wir in No. 236 betrachtet haben, und deren Ausdruck folgender ist:

$$P = (x_1 - x_0)(x_2 - x_0) \ldots (x_{n-1} - x_0)(x_2 - x_1) \ldots (x_{n-1} - x_{n-2}).$$

Es liegt auf der Hand, dass die Functionen, welche zwei verschiedene Werthe haben, alle cyclischen Substitutionen dritter

Ordnung, die sich aus den Veränderlichen bilden lassen, aber keine Transposition zulassen.

Man kann sich die Aufgabe stellen, die einfachsten der Functionen zu bestimmen, welche einem gegebenen Systeme conjugirter Substitutionen entsprechen, z. B. diejenigen rationalen und ganzen Functionen, welche den niedrigsten Grad haben. So ausgesprochen macht die vorliegende Aufgabe Betrachtungen ganz anderer Art erforderlich, und ihre Lösung bietet grosse Schwierigkeiten. Wir werden diese neue Aufgabe hier nicht in Angriff nehmen, zumal dieselbe ganz ausserhalb unseres Gegenstandes liegt. Um jedoch eine Anwendung der Theorie zu machen, die wir in den vorhergehenden Kapiteln entwickelt haben, wollen wir ein besonderes Verfahren darlegen, welches sehr leicht die Functionen liefert, die gewissen Systemen conjugirter Substitutionen entsprechen.

Wenn ein System conjugirter Substitutionen $m$mal transitiv ist, so werden wir mit Cauchy sagen, die Functionen, welche diese Substitutionen zulassen, seien $m$mal transitiv.

Zweimal transitive Functionen von n Veränderlichen, welche $1 . 2 . 3 \ldots (n-2)$ Werthe haben. n wird als Primzahl vorausgesetzt.

482. Die Functionen, um die es sich hier handelt, spielen in der Theorie der algebraischen Gleichungen eine wichtige Rolle. Sie entsprechen dem conjugirten Systeme, welches aus den $n(n-1)$ linearen und ganzen Substitutionen von der Form

$$\binom{az+b}{z}$$

gebildet ist; darin bezeichnet z der Reihe nach alle Indices $0, 1, 2, \ldots, (n-1)$ der n Veränderlichen

$$(1). \qquad x_0, x_1, x_2, \ldots, x_{n-1},$$

und die Werthe von $az+b$ werden in Beziehung auf den Modul n zwischen den Grenzen 0 und $n-1$ genommen.

Es sei α eine Wurzel der Gleichung

$$(2). \qquad \frac{x^n-1}{x-1} = 0,$$

und es werde

(3). $$t = x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1}$$
gesetzt: dann ist t offenbar eine Function der n Veränderlichen (1), welche $1 . 2 . 3 \ldots n$ verschiedene Werthe hat.

Führt man an t die Substitution n^{ter} Ordnung
$$\binom{z+1}{z}$$
und die verschiedenen Potenzen dieser Substitution aus, so erhält man n Resultate

(4). $$t_0 , t_1 , t_2 , \ldots , t_{n-1} ,$$
und weil t_μ aus t dadurch hervorgeht, dass jeder Index z durch $z + \mu$ ersetzt wird, so hat man
$$t_\mu = x_\mu + \alpha x_{\mu+1} + \cdots + \alpha^j x_{\mu+j} + \cdots + \alpha^{n-1} x_{\mu+n-1}.$$
Ist
$$\mu + j \equiv i \text{ oder } j \equiv i - \mu \ (mod.\ n) ,$$
wo i zwischen 0 und $n - 1$ liegt, so folgt
$$t_\mu = \alpha^{-\mu} (x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1}) ,$$
oder
$$t_\mu = \alpha^{-\mu} t.$$
Jede der Functionen (4) ist danach gleich dem Produkte von t in eine Potenz von α, und da man
$$\alpha^n = 1$$
hat, so haben alle diese Functionen dieselbe n^{te} Potenz. Setzt man also $\vartheta = t^n$, oder

(5). $$\vartheta = (x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1})^n ,$$
so erleidet die Function ϑ durch die cyclische Substitution
$$\binom{z+1}{z}$$
keine Aenderung, und die Anzahl ihrer verschiedenen Werthe ist offenbar
$$1 . 2 . 3 \ldots (n - 1).$$
Wir bezeichnen jetzt mit r eine primitive Wurzel der Primzahl n und führen an den Indices z der Veränderlichen x die Potenzen $0 , 1 , 2 , \ldots , (n - 2)$ der cyclischen Substitution $(n - 1)^{\text{ter}}$ Ordnung
$$\binom{rz}{z}$$
aus; auf diese Weise erhalten wir $n - 1$ Resultate, die wir durch

(6). $$\vartheta_0\,,\,\vartheta_1\,,\,\vartheta_2\,,\,\ldots\,,\,\vartheta_{n-2}$$
darstellen wollen. Es ist allgemein
$$\vartheta_\mu = (x_0 + \alpha x_{r^\mu} + \cdots + \alpha^j x_{jr^\mu} + \cdots)^n,$$
und wenn man
$$j r^\mu \equiv i\,,\, j \equiv i r^{n-1-\mu} \ (mod.\ n)$$
setzt, wo i zwischen 0 und $n-1$ liegt, so ergiebt sich
$$\vartheta_\mu = (x_0 + \cdots + \alpha^{ir^{n-1-\mu}} x_i + \cdots)^n;$$
daraus folgt, dass ϑ_μ aus ϑ hervorgeht, wenn α durch $\alpha^{r^{n-1-\mu}}$ ersetzt wird. Ertheilt man nun μ der Reihe nach die Werthe
$$0\,,\,1\,,\,2\,,\,\ldots\,,\,(n-2)\,,$$
so nimmt $r^{n-1-\mu}$ in Beziehung auf den Modul n alle Werthe
$$1\,,\,2\,,\,3\,,\,\ldots\,,\,(n-1)$$
an, und folglich liefert der Ausdruck $\alpha^{r^{n-1-\mu}}$ der Reihe nach die $n-1$ Wurzeln

(7). $$\alpha\,,\,\beta\,,\,\gamma\,,\,\ldots\,,\,\omega$$
der Gleichung (2). Man erhält mithin die Werthe der Functionen (6), wenn man in dem Ausdrucke von ϑ α durch jede der Wurzeln (7) ersetzt, d. h. es ist

(8). $$\begin{cases} \vartheta_0 = (x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1})^n, \\ \vartheta_1 = (x_0 + \beta x_1 + \beta^2 x_2 + \cdots + \beta^{n-1} x_{n-1})^n, \\ \vartheta_2 = (x_0 + \gamma x_1 + \gamma^2 x_2 + \cdots + \gamma^{n-1} x_{n-1})^n, \\ \ldots\ldots\ldots\ldots\ldots\ldots, \\ \vartheta_{n-2} = (x_0 + \omega x_1 + \omega^2 x_2 + \cdots + \omega^{n-1} x_{n-1})^n. \end{cases}$$

Keine der Functionen (8) erleidet durch die Substitution $\binom{z+1}{z}$ eine Aenderung, und bei Anwendung der Substitution $\binom{rz}{z}$ gehen dieselben ineinander über. Bezeichnet also ϑ eine unbestimmte Grösse, so lässt die Function
$$(\vartheta - \vartheta_0)\,(\vartheta - \vartheta_1)\,(\vartheta - \vartheta_2)\,\cdots\,(\vartheta - \vartheta_{n-2})$$
die Substitutionen
$$\binom{z+1}{z}\ ,\ \binom{rz}{z},$$
folglich auch alle linearen und ganzen Substitutionen
$$\binom{\lambda z}{z}$$

zu, und die Anzahl ihrer verschiedenen Werthe ist

$$1 \,.\, 2 \,.\, 3 \ldots (n - 2).$$

Es liegt auf der Hand, dass alle symmetrischen Functionen von $\vartheta_0, \vartheta_1, \ldots, \vartheta_{n-2}$ die linearen und ganzen Substitutionen zulassen; diese Functionen sind daher zweimal transitiv.

483. Bezeichnet man mit d einen Divisor von $n-1$, macht

$$n - 1 = de$$

und wendet auf die Function ϑ die Potenzen der regelmässigen Substitution e^{ter} Ordnung

$$\begin{pmatrix} r^d z \\ z \end{pmatrix}$$

an, so erhält man e Resultate

$$\vartheta_0, \vartheta_1, \vartheta_2, \ldots, \vartheta_{e-1},$$

und es ist klar, dass die Function

$$(\vartheta - \vartheta_0)(\vartheta - \vartheta_1) \ldots (\vartheta - \vartheta_{e-1})$$

$1 \,.\, 2 \,.\, 3 \ldots (n-2) \times d$ verschiedene Werthe hat.

Dreimal transitive Functionen von $n + 1$ Veränderlichen, welche $1 \,.\, 2 \,.\, 3 \ldots (n-2)$ Werthe haben. n ist eine Primzahl.

484. Die Existenz der in Rede stehenden Functionen ist *a priori* einleuchtend; dieselben entsprechen dem conjugirten Systeme, welches aus den $(n+1)\,n\,(n-1)$ auf den Modul n bezüglichen linearen Substitutionen besteht. Die Regel, welche ich für die Bildung dieser Functionen darlegen werde, unterscheidet sich nur in der Form von derjenigen, die zuerst Émile Mathieu gegeben hat.

Wir betrachten zunächst die n Veränderlichen

$$(1). \qquad x_0, x_1, x_2, \ldots, x_{n-1},$$

und setzen, wie in No. 482,

$$(2). \qquad \begin{cases} \vartheta_0 = (x_0 + \alpha\, x_1 + \alpha^2\, x_2 + \cdots + \alpha^{n-1}\, x_{n-1})^n, \\ \vartheta_1 = (x_0 + \beta\, x_1 + \beta^2\, x_2 + \cdots + \beta^{n-1}\, x_{n-1})^n, \\ \ldots\ldots\ldots\ldots\ldots\ldots, \\ \vartheta_{n-2} = (x_0 + \omega\, x_1 + \omega^2\, x_2 + \cdots + \omega^{n-1}\, x_{n-1})^n, \end{cases}$$

wo $\alpha, \beta, \gamma, \ldots, \omega$ die $n-1$ Wurzeln der Gleichung

$$\frac{x^n - 1}{x - 1} = 0$$

sind. Es sei v irgend eine rationale und symmetrische Function der $n-1$ Ausdrücke (2); diese Function v erleidet, wie wir gesehen haben, durch keine Substitution von der Form

(3). $$\begin{pmatrix} \lambda z \\ z \end{pmatrix},$$

wo λz irgend eine ganze Function des Index z ist, eine Aenderung.

Der Theorie der ähnlichen Functionen zufolge ist jede Function der Veränderlichen (1), welche die Substitutionen (3) zulässt, eine rationale Function von v, in welcher die Coefficienten der Potenzen von v symmetrische Functionen sind. Bezeichnen wir also mit V_0 eine beliebige rationale Function der Grösse v und einer neuen Veränderlichen, die wir durch x_∞ darstellen wollen, so ist V_0 eine Function der $n+1$ Veränderlichen

$$x_0, x_1, x_2, \ldots, x_{n-1}, x_\infty,$$

welche durch keine ganze und lineare Substitution verändert wird; man kann für V_0, wenn man will, die Function v selbst nehmen.

Dies vorausgesetzt, sei ϑz eine rationale lineare Function $(n+1)^{\text{ter}}$ Ordnung für den Modul n, und es werde mit V_i der Werth bezeichnet, welchen V_0 annimmt, wenn man an dieser Function i mal die Substitution

$$\begin{pmatrix} \vartheta z \\ z \end{pmatrix}$$

vollzieht; wir drücken dies nach Cauchy's Bezeichnungsart dadurch aus, dass wir schreiben:

(4). $$V_i = \begin{pmatrix} \vartheta^i z \\ z \end{pmatrix} V_0.$$

Ferner sei ωz eine rationale lineare Function von einer beliebigen Ordnung für den Modul n, und es werde an V_i die Substitution

$$\begin{pmatrix} \omega z \\ z \end{pmatrix}$$

ausgeführt; man erhält ein Resultat, welches durch

$$\binom{\omega z}{z} V_i = \binom{\omega\vartheta^i z}{z} V_0$$

dargestellt werden kann. Wenn nun j irgend eine ganze Zahl bezeichnet, so kann man, da die Function ϑz von der Ordnung $n+1$ ist, die Substitution

$$\binom{\omega\vartheta^i z}{z}$$

dadurch ausführen, dass man zunächst die Substitution

$$\binom{\vartheta^j \omega \vartheta^i z}{z},$$

sodann die Substitution

$$\binom{\vartheta^{n+1-j} z}{z}$$

vollzieht. Man kann daher

$$\binom{\omega z}{z} V_i = \binom{\vartheta^{n+1-j} z}{z} \binom{\vartheta^j \omega\vartheta^i z}{z} V_0$$

schreiben, und hierin ist jede der Zahlen i, j willkürlich. Nach dem Lehrsatze der No. 472 entspricht aber jedem Werthe der einen der Zahlen i, j ein solcher Werth der andern, dass

$$\binom{\vartheta^j \omega\vartheta^i z}{z}$$

eine ganze Substitution ist. Wenn ausserdem eine dieser Zahlen i, j der Reihe nach die $n+1$ Werthe $0, 1, 2, \ldots, n$ erhält, so nimmt auch die andere alle diese Werthe an. Werden also i und j so gewählt, dass die Bedingungen des eben erwähnten Lehrsatzes erfüllt sind, so hat man, da V_0 durch die linearen und ganzen Substitutionen keine Aenderung erleidet,

$$\binom{\omega z}{z} V_i = \binom{\vartheta^{n+1-j} z}{z} V_0,$$

oder nach Formel (4)

$$(5). \qquad \binom{\omega z}{z} V_i = V_{n+1-j}.$$

Wir machen nochmals darauf aufmerksam, dass, wenn in dieser Formel die eine der Zahlen i, j der Reihe nach die $n+1$ Werthe $0, 1, 2, \ldots, n$ erhält, auch die andere eben dieselben Werthe annehmen wird.

Die Formel (5) liefert das wichtige Resultat, dass die $n+1$ Functionen

$$(6). \qquad V_0, V_1, V_2, \ldots, V_n$$

ein System bilden, welches durch keine lineare Substitution verändert wird, d. h. dass eine solche Substitution die Functionen (6) nur gegeneinander vertauschen kann.

Bezeichnet daher T eine symmetrische Function der Ausdrücke (6), macht man z. B.

$$(7). \qquad T = (V - V_0)(V - V_1) \ldots (V - V_n),$$

wo V eine unbestimmte Grösse ist, so wird die Function T alle linearen Substitutionen zulassen; sie ist also dreimal transitiv und hat $1.2.3\ldots(n-2)$ verschiedene Werthe.

Bezeichnet man mit T_1 und T_2 zwei Functionen, welche T ähnlich sind, mit P die alternirende Function

$$(x_1 - x_0) \ldots (x_1 - x_\infty)(x_2 - x_1) \ldots (x_\infty - x_{n-1})$$

der $n+1$ Veränderlichen, und macht

$$S = T_1 + PT_2,$$

so lässt die Function S alle linearen Substitutionen zu, deren Determinante quadratischer Rest von n ist, welche folglich einer geraden Anzahl von Transpositionen äquivalent sind. S hat daher, wie Mathieu bemerkt hat, $2 \times 1.2\ldots(n-2)$ verschiedene Werthe. Man kann die Functionen S ebenso wie die Functionen T bilden, indem man sich des Zusatzes der No. 472 bedient; wir müssen uns aber auf diese Andeutung beschränken.

Ueber die dreimal transitiven Functionen von sechs Veränderlichen, welche sechs verschiedene Werthe haben.

485. Man kann den Functionen, mit denen wir uns soeben beschäftigt haben, mehrere verschiedene Formen geben. Als Beispiel nehmen wir den Fall der transitiven Functionen von sechs Buchstaben, welche sechs verschiedene Werthe haben.

Wir bezeichnen die Veränderlichen mit

$$x_0, x_1, x_2, x_3, x_4, x_\infty,$$

setzen

$$V_0 = x_\infty x_0 + x_1 x_4 + x_2 x_3,$$

und führen an V_0 die Potenzen der Substitution 5ter Ordnung

$$\binom{z+1}{z} = (0\,,\,1\,,\,2\,,\,3\,,\,4)$$

aus, indem wir die Indices z in Beziehung auf den Modul 5 nehmen. Es ergeben sich folgende Resultate:

$$\begin{cases} V_0 = x_\infty\, x_0 + x_1\, x_4 + x_2\, x_3\,, \\ V_1 = x_\infty\, x_1 + x_2\, x_0 + x_3\, x_4\,, \\ V_2 = x_\infty\, x_2 + x_3\, x_1 + x_4\, x_0\,, \\ V_3 = x_\infty\, x_3 + x_4\, x_2 + x_0\, x_1\,, \\ V_4 = x_\infty\, x_4 + x_0\, x_3 + x_1\, x_2\,. \end{cases}$$

Macht man sodann

$$T = (V - V_0)\,(V - V_1)\,(V - V_2)\,(V - V_3)\,(V - V_4),$$

wo V eine unbestimmte Grösse ist, so lassen alle linearen und ganzen Substitutionen die Function T ungeändert, und da dieselbe nicht symmetrisch ist, so hat sie genau sechs verschiedene Werthe. Zur Begründung dieser Behauptung genügt es, zu zeigen, dass T keine Aenderung durch zwei lineare Substitutionen erleidet, von denen die eine die Ordnung 4, die andere die Ordnung 6 hat. Die Substitution 4ter Ordnung

$$\binom{2\,z}{z} = (1\,,\,2\,,\,4\,,\,3)$$

lässt V_0 unverändert und verwandelt

$$V_1\,,\; V_2\,,\; V_3\,,\; V_4$$

in

$$V_2\,,\; V_4\,,\; V_1\,,\; V_3\,.$$

Ferner verwandelt die Substitution 6ter Ordnung

$$\left(\begin{matrix}\binom{z+3}{z} \\ z\end{matrix}\right) = (0\,,\,\infty\,,\,1\,,\,4\,,\,3\,,\,2)$$

$$V_0\,,\; V_1\,,\; V_2\,,\; V_3\,,\; V_4$$

in

$$V_1\,,\; V_0\,,\; V_3\,,\; V_4\,,\; V_2\,,$$

und damit ist unser Satz bewiesen.

Lagrange's Methode, eine Function der Wurzeln einer gegebenen Gleichung zu berechnen, wenn man irgend eine andere Function der Wurzeln kennt.

486. Eine der wichtigsten Arbeiten, die seit einem Jahrhundert über die algebraische Theorie der Gleichungen veröffent-

licht sind, ist unstreitig die berühmte Abhandlung von Lagrange, die wir bereits in No. 189 zu erwähnen hatten, und die in den Mémoires de l'Académie de Berlin (1770 und 1771) enthalten ist. Man findet in dieser grossen Arbeit ausser anderen bemerkenswerthen Resultaten den folgenden schönen Lehrsatz:

Sobald man auf irgend eine Weise den Werth einer rationalen Function der Wurzeln einer Gleichung gefunden hat, kann man im Allgemeinen den Werth einer beliebigen anderen rationalen Function eben derselben Wurzeln bestimmen, und zwar vermittels einer linearen Gleichung. Einige besondere Fälle machen indess die Auflösung einer Gleichung zweiten, dritten, u. s. w. Grades erforderlich.

Es seien

$$x_0\,,\; x_1\,,\; \ldots\,,\; x_{n-1}$$

die n Wurzeln der Gleichung

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \cdots + p_{n-1} x + p_n = 0\,, \tag{1}$$

und

$$V = F(x_0\,, x_1\,, \ldots\,, x_{n-1})\,,$$
$$y = f\,(x_0\,, x_1\,, \ldots\,, x_{n-1})$$

zwei rationale Functionen dieser Wurzeln, von denen die erste einen gegebenen Werth hat.

Wir setzen zunächst voraus, die Function f lasse alle Substitutionen von F zu. In diesem Falle kann man den Werth von f durch Anwendung der Methode bestimmen, deren wir uns in No. 480 bedient haben. Stellt man nämlich durch

$$V_0\,,\; V_1\,,\; V_2\,,\; \ldots\,,\; V_{\nu-1} \tag{2}$$

die verschiedenen Werthe, welche F in Folge der Substitutionen annimmt, und durch

$$y_0\,,\; y_1\,,\; y_2\,,\; \ldots\,,\; y_{\nu-1} \tag{3}$$

die entsprechenden Werthe von f dar, und setzt, wie in No. 480,

$$\left\{\begin{array}{l} y_0 + y_1 + y_2 + \cdots + y_{\nu-1} = t_0\,, \\ V_0 y_0 + V_1 y_1 + V_2 y_2 + \cdots + V_{\nu-1} y_{\nu-1} = t_1\,, \\ V_0^2 y_0 + V_1^2 y_1 + V_2^2 y_2 + \cdots + V_{\nu-1}^2 y_{\nu-1} = t_2\,, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ V_0^{\nu-1} y_0 + V_1^{\nu-1} y_1 + V_2^{\nu-1} y_2 + \cdots + V_{\nu-1}^{\nu-1} y_{\nu-1} = t_{\nu-1}\,, \end{array}\right. \tag{4}$$

so kann man die Grössen $t_0, t_1, \ldots, t_{\nu-1}$ durch die bekannten Grössen ausdrücken, da dieselben symmetrische Functionen der Wurzeln der Gleichung (1) sind. Sodann lehrt die Auflösung der Gleichungen (4) die Unbekannten $y_0, y_1, \ldots$ kennen.

Stellt man durch

$$(5).\qquad \psi(V) = V^{\nu-1} + P_1 V^{\nu-2} + \cdots + P_{\nu-1} V + P_\nu$$

das Polynom dar, welches gleich dem Produkte

$$(V - V_0)(V - V_1) \ldots (V - V_{\nu-1})$$

ist, durch $\psi'(V)$ die Abgeleitete von $\psi(V)$, und macht der Kürze wegen

$$(6).\qquad \begin{cases} s_{\nu-1} = t_{\nu-1} + P_1 t_{\nu-2} + P_2 t_{\nu-3} + \cdots + P_{\nu-2} t_1 + P_{\nu-1} t_0, \\ s_{\nu-2} = t_{\nu-2} + P_1 t_{\nu-3} + P_2 t_{\nu-4} + \cdots + P_{\nu-2} t_0, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ s_1 \;\;= t_1 \;\;+ P_1 t_0, \\ s_0 \;\;= t_0, \end{cases}$$

sowie

$$(7).\qquad \Theta(V) = s_0 V^{\nu-1} + s_1 V^{\nu-2} + \cdots + s_{\nu-2} V + s_{\nu-1},$$

so sind, wie wir gesehen haben, die Werthe der Unbekannten y:

$$(8).\qquad y_0 = \frac{\Theta(V_0)}{\psi'(V_0)},\; y_1 = \frac{\Theta(V_1)}{\psi'(V_1)},\; \ldots,\; y_{\nu-1} = \frac{\Theta(V_{\nu-1})}{\psi'(V_{\nu-1})}.$$

Unter der Voraussetzung, die wir gemacht haben, hat die Function F ν a l g e b r a i s c h verschiedene Werthe. Hier sind aber $x_0, x_1, \ldots, x_{n-1}$ nicht mehr unbestimmte Grössen, und es kann vorkommen, dass einige der Grössen (2) n u m e r i s c h gleich sind. Wenn dieser Fall eintritt, so besitzt die Gleichung

$$(9).\qquad \psi(V) = 0$$

vielfache Wurzeln, und einige der Formeln (8) werden illusorisch. Wenn aber V_ϱ eine einfache Wurzel der Gleichung (9) ist, so liefert die Formel

$$y_\varrho = \frac{\Theta(V_\varrho)}{\psi'(V_\varrho)}$$

in allen Fällen, wie wir jetzt zeigen wollen, den Werth von y, welcher dem Werthe V_ϱ von V entspricht.

487. Aus dem Vorhergehenden ist ersichtlich, dass wir die Betrachtung der No. 480 zu vervollständigen haben, um sie auf den hier vorliegenden Fall anwendbar zu machen. Wir nehmen

an, i der Grössen (2) seien numerisch verschieden, und stellen dieselben durch

(10). $$V_0\,,\ V_1\,,\ V_2\,,\ \ldots\,,\ V_{i-1}$$

dar. Es seien V_ϱ eine der Grössen (10) und Y_ϱ die Summe aller Werthe von y, welche den Werthen von V entsprechen, die gleich V_ϱ sind. Die Gleichungen (4) gehen über in

(11). $$\left\{\begin{array}{l} Y_0 + Y_1 + \cdots + Y_{i-1} = t_0\,, \\ V_0\,Y_0 + V_1\,Y_1 + \cdots + V_{i-1}\,Y_{i-1} = t_1\,, \\ \ldots\ldots\ldots\ldots\ldots, \\ V_0^{i-1}\,Y_0 + V_1^{i-1}\,Y_1 + \cdots + V_{i-1}^{i-1}\,Y_{i-1} = t_{i-1}\,, \\ \ldots\ldots\ldots\ldots\ldots, \\ V_0^{\nu-1}\,Y_0 + V_1^{\nu-1}\,Y_1 + \cdots + V_{i-1}^{\nu-1}\,Y_{i-1} = t_{\nu-1}\,. \end{array}\right.$$

Diese Gleichungen (11) können offenbar nur die i Grössen

$$Y_0\,,\ Y_1\,,\ \ldots\,,\ Y_{i-1}$$

bestimmen, und zu diesem Zwecke reichen die i ersten Gleichungen völlig aus. Wir werden trotzdem eine grössere Anzahl anwenden, um zu Formeln zu gelangen, in denen nur die beiden bereits eingeführten Functionen $\Theta(V)$, $\psi(V)$ vorkommen.

Wir bezeichnen mit r die Anzahl der Grössen (2), welche gleich V_ϱ sind, und betrachten die $\nu - r + 1$ ersten Gleichungen (11). Im Falle $r = 1$ wird keine Gleichung ausgeschlossen. Addirt man die angegebenen Gleichungen, nachdem man sie mit den Factoren

$$\vartheta_0\,,\ \vartheta_1\,,\ \ldots\,,\ \vartheta_{\nu-r-1}\,,\ 1$$

multiplicirt hat, und macht der Kürze wegen

(12). $$\varphi(V) = V^{\nu-r} + \vartheta_{\nu-r-1}\,V^{\nu-r-1} + \cdots + \vartheta_1\,V + \vartheta_0\,,$$

so ergiebt sich

$$\begin{gathered} Y_0\,\varphi(V_0) + Y_1\,\varphi(V_1) + \cdots + Y_{i-1}\,\varphi(V_{i-1}) \\ = \vartheta_0\,t_0 + \vartheta_1\,t_1 + \cdots + \vartheta_{\nu-r-1}\,t_{\nu-r-1} + t_{\nu-r}\,, \end{gathered}$$

und wenn die Factoren ϑ in der Weise bestimmt werden, dass man identisch

$$\varphi(V) = \frac{\psi(V)}{(V - V_\varrho)^r}$$

hat, so liefert die vorhergehende Gleichung

$$(13).\quad Y_\varrho = \frac{\vartheta_0 t_0 + \vartheta_1 t_1 + \cdots + \vartheta_{\nu-r-1} t_{\nu-r-1} + t_{\nu-r}}{\varphi(V_\varrho)}.$$

Der Ausdruck von $\varphi(V)$ wird leicht dadurch erhalten, dass man die beiden Ausdrücke

$$\psi(V) = V^\nu + P_1 V^{\nu-1} + \cdots + P_{\nu-1} V + P_\nu,$$

$$\frac{1}{(V-V_\varrho)^r} = \frac{1}{V^r} + \frac{r}{1} \cdot \frac{V_\varrho}{V^{r+1}} + \frac{r(r+1)}{1.2} \cdot \frac{V_\varrho^2}{V^{r+2}} + \cdots$$

mit einander multiplicirt und in dem Produkte die negativen Potenzen von V vernachlässigt. Vergleicht man das erhaltene Resultat mit der Formel (12), so ergiebt sich

$$(14).\left\{\begin{aligned} \vartheta_0 &= P_{\nu-r} + \frac{r}{1} P_{\nu-r-1} V_\varrho + \frac{r(r+1)}{1.2} P_{\nu-r-2} V_\varrho^2 + \cdots \\ &\quad + \frac{r(r+1)\ldots(\nu-1)}{1.2\ldots(\nu-r-1)} V_\varrho^{\nu-r}, \\ \vartheta_1 &= P_{\nu-r-1} + \frac{r}{1} P_{\nu-r-2} V_\varrho + \cdots \\ &\quad + \frac{r(r+1)\ldots(\nu-2)}{1.2\ldots(\nu-r-2)} V_\varrho^{\nu-r-1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ \vartheta_{\nu-r-2} &= P_2 + \frac{r}{1} P_1 V_\varrho + \frac{r(r+1)}{1.2} V_\varrho^2, \\ \vartheta_{\nu-r-1} &= P_1 + \frac{r}{1} V_\varrho. \end{aligned}\right.$$

Aus den Formeln (14) und (6) geht hervor, dass der Zähler des Ausdrucks (13) von Y_ϱ das Produkt des numerischen Factors

$$\frac{1}{1.2.3\ldots(r-1)}$$

in das Polynom

$$(15).\quad \left\{\begin{aligned} &(\nu-1)\ldots(\nu-r)\, s_0\, V_\varrho^{\nu-r} \\ &\quad + (\nu-2)\ldots(\nu-r-1)\, s_1\, V_\varrho^{\nu-r-1} + \cdots \\ &\quad + r(r-1)\ldots 2\, s_{\nu-r} \end{aligned}\right.$$

ist, und dieser Ausdruck (15) ist augenscheinlich der Werth, welchen die $(r-1)^{\text{te}}$ Abgeleitete, $\Theta^{r-1}(V)$, des Polynoms $\Theta(V)$ für $V = V_\varrho$ annimmt. Der Nenner des Ausdrucks von Y_ϱ ist gleich $\varphi(V_\varrho)$ oder gleich

$$\frac{\psi^r(V_\varrho)}{1.2.3\ldots r},$$

und die Formel (13) geht somit über in

$$(16).\quad \frac{1}{r} Y_\varrho = \frac{\Theta^{r-1}(V_\varrho)}{\psi^r(V_\varrho)}.$$

Wenn $r = 1$ ist, so muss Y_ϱ durch y_ϱ und $\Theta^{r-1}(V_\varrho)$ durch

$\Theta(V_\varrho)$ ersetzt werden; man gelangt auf diese Weise wieder zu derjenigen der Formeln (8), welche y_ϱ bestimmt,

Die Formel (16) liefert das wichtige Resultat, dass in allen Fällen

$$y = \frac{\Theta(V)}{\psi'(V)}$$

ist, vorausgesetzt dass man, wenn sich das zweite Glied für $V = V_\varrho$ auf $\frac{0}{0}$ reducirt, die beiden Termen gemeinschaftlichen Factoren $V - V_\varrho$ unterdrückt, ehe man $V = V_\varrho$ macht, und dass man ferner y durch das arithmetische Mittel der Werthe ersetzt, welche dem Werthe V_ϱ entsprechen.

Sind

$$y_0, y_1, y_2, \ldots, y_{r-1}$$

die r Werthe von y, welche dem Werthe V_ϱ entsprechen, so ermöglicht es die im Vorstehenden dargelegte Methode, die Summe

$$y_0 + y_1 + y_2 + \cdots + y_{r-1}$$

zu berechnen. Auf dieselbe Weise kann man die Summe der Quadrate dieser Grössen, die Summe ihrer Cuben, u. s. w., endlich die Summe ihrer r^{ten} Potenzen bestimmen. Man kann also die Gleichung r^{ten} Grades bilden, welche die Grössen $y_0, y_1, \ldots, y_{r-1}$ zu Wurzeln hat. Wenn also die Gleichung in V gleiche Wurzeln hat, so kann die Bestimmung der Function y von einer Gleichung zweiten, oder dritten, oder u. s. w. Grades abhängen.

488. Unsere Betrachtung lässt sich auch auf den Fall ausdehnen, in welchem die Function y nicht alle Substitutionen der gegebenen Function V zulässt.

In diesem Falle ist die Anzahl ν der verschiedenen Werthe von V kleiner als $N = 1.2\ldots n$, und wenn man $N = \mu\nu$ setzt, so vertheilen sich die N Werthe von V in ν Gruppen, deren jede μ gleiche Werthe enthält.

Es seien

$$\begin{array}{llll} V_0, & V_0^{(1)}, & \ldots, & V_0^{(\mu-1)}, \\ V_1, & V_1^{(1)}, & \ldots, & V_1^{(\mu-1)}, \\ \ldots & \ldots & \ldots & \ldots, \\ V_{\nu-1}, & V_{\nu-1}^{(1)}, & \ldots, & V_{\nu-1}^{(\mu-1)} \end{array}$$

diese ν Gruppen und $y_\varrho^{(\sigma)}$ der Werth von y, welcher $V_\varrho^{(\sigma)}$ entspricht.

Bezeichnet z irgend eine rationale und symmetrische Function der Grössen

$$y_\varrho\,,\; y_\varrho^{(1)}\,,\;\ldots\,,\; y_\varrho^{(\mu-1)},$$

so lässt z offenbar alle Substitutionen von V_ϱ zu; man kann daher z im Allgemeinen rational durch V_ϱ ausdrücken. Hat man auf diese Weise μ symmetrische Functionen der Grössen

$$y_\varrho\,,\; y_\varrho^{(1)}\,,\;\ldots\,,\; y_\varrho^{(\mu-1)}$$

berechnet, so kann man die Gleichung μ^{ten} Grades bilden, welche diese μ Werthe von y zu Wurzeln hat.

489. Aus dem Vorhergehenden ergiebt sich, dass man immer die n Wurzeln $x_0\,, x_1\,, \ldots x_{n-1}$ einer gegebenen Gleichung n^{ten} Grades bestimmen kann, wenn man den Werth einer Function V dieser Wurzeln kennt, vorausgesetzt dass die $1.2.3\ldots n$ Werthe, welche V in Folge der Vertauschungen der Wurzeln annimmt, nicht nur in Beziehung auf die algebraische Form, sondern auch numerisch von einander verschieden sind.

Man kann nämlich voraussetzen, die unbekannte Function y reducire sich auf irgend eine der Wurzeln, z. B. auf x_0; dann lässt sich x_0 rational durch V und die Coefficienten der vorgelegten Gleichung ausdrücken. Nimmt man weiter an, y reducire sich auf eine andere Wurzel x_1, so kann man x_1 als rationale Function von V darstellen, u. s. w. Es geht daraus hervor, dass wenn der gegebene Werth von V kommensurabel, d. h. rational durch die als bekannt angesehenen Grössen ausdrückbar ist, die Wurzeln der vorgelegten Gleichung sämmtlich kommensurabel sein werden.

Sind dagegen nicht alle Werthe von V von einander verschieden, nimmt diese Function z. B. in Folge der Substitutionen, welchen die Werthe

$$x_0\,,\; x_1\,,\;\ldots\,,\; x_{k-1}$$

der Function $y = x$ entsprechen, k gleiche Werthe an, so lehrt unsere Methode nicht diese Wurzeln selbst kennen, sondern ermöglicht es nur, die Gleichung k^{ten} Grades zu bilden, von welcher dieselben abhängen.

Die Theorie, die wir hier dargelegt haben, umfasst alle allgemeineren Resultate, welche über die Graderniedrigung der Gleichungen bekannt sind, zwischen deren Wurzeln eine gegebene Relation besteht; denn dieser Fall ist offenbar derselbe wie derjenige, in welchem man den Werth einer Function der Wurzeln kennt.

Untersuchungen von Galois, die sich auf die vorhergehende Theorie beziehen.

490. Die vorstehende Untersuchung hat uns zu einem Lehrsatze von unverkennbarer Wichtigkeit geführt, der sich folgendermassen aussprechen lässt:

Lehrsatz. — Es sei

(1). $$f(x) = 0$$

irgend eine Gleichung n^{ten} Grades, deren n Wurzeln

$$x_0\,,\ x_1\,,\ x_2\,,\ \ldots\,,\ x_{n-1}$$

ungleich sind; ferner sei

$$V = \varphi\,(x_0\,,\ x_1\,,\ \ldots\,,\ x_{n-1})$$

eine rationale Function dieser Wurzeln, die so gewählt ist, dass die $1\,.\,2\,.\,3\ldots n$ Werthe, welche sie in Folge der Substitutionen der Wurzeln annimmt, sämmtlich von einander verschieden sind: dann lassen sich die n Wurzeln $x_0, x_1, \ldots, x_{n-1}$ rational durch V ausdrücken.

Es dürfte von Nutzen sein, hier den Beweis mitzutheilen, den Galois (Journal de Mathématiques pures et appliquées, t. XI) für diesen Lehrsatz gegeben hat.

Wir bezeichnen mit V_0 den gegebenen Werth von V und mit

$$V_0\,,\ V_1\,,\ \ldots\,,\ V_{\mu-1}$$

die $\mu = 1\,.\,2\,.\,3\ldots(n-1)$ Werthe, welche V in Folge der Substitutionen der $n-1$ Wurzeln

$$x_1\,,\ x_2\,,\ \ldots\,,\ x_{n-1}$$

annimmt. Man hat dann eine Gleichung μ^{ten} Grades in V, nämlich

(2). $$(V - V_0)\,(V - V_1)\ldots(V - V_{\mu-1}) = 0\,,$$

deren Wurzeln $V_0, V_1, \ldots$ sämmtlich von einander verschieden sind, und deren Coefficienten, als symmetrische Functionen der Wurzeln $x_1, x_2, \ldots, x_{n-1}$ der Gleichung

$$\frac{f\,(x)}{x - x_0} = 0\,,$$

sich rational durch die Coefficienten dieser Gleichung, d. h. rational durch x_0 und die Coefficienten der vorgelegten Gleichung (1) ausdrücken lassen. Die Gleichung (2) kann somit auf die Form

(3). $$F\,(V\,,\ x_0) = 0$$

gebracht werden, in welcher F eine rationale Function von V

und von x_0 bezeichnet. Nun wird der Gleichung (2) oder (3) durch den Werth $V = V_0$ genügt; man hat daher identisch

$$F(V_0, x_0) = 0,$$

so dass die Gleichung

(4). $$F(V_0, x) = 0$$

durch

$$x = x_0$$

befriedigt wird; die Gleichungen (1) und (4) haben somit eine Wurzel x_0 gemeinschaftlich. Wir behaupten ferner, dass diese Gleichungen keine zweite Wurzel gemeinschaftlich haben können. Wird nämlich der Gleichung (4) durch $x = x_1$ genügt, so ist identisch

$$F(V_0, x_1) = 0;$$

folglich hat die Gleichung

(5). $$F(V, x_1) = 0$$

die Wurzel $V = V_0$. Nun geht die Gleichung (5) aus (3) oder aus (2) durch die Transposition der Wurzeln x_0 und x_1 hervor; ausserdem verwandelt diese Transposition die Grössen

$V_0, V_1, \ldots, V_{\mu-1}$ in andere $V_0', V_1', \ldots, V_{\mu-1}'$,

welche der Voraussetzung nach von den ersteren sämmtlich verschieden sind; die Gleichung (5) kann also auf die Form

$$(V - V_0')(V - V_1') \ldots (V - V_{\mu-1}') = 0$$

gebracht werden, und daraus ist ersichtlich, dass sie nicht die Wurzel V_0 haben kann.

Da die Gleichungen (1) und (4) nur die Wurzel x_0 gemeinschaftlich haben, so ist es leicht, diese Wurzel zu bestimmen. Man hat zu diesem Zwecke den grössten gemeinschaftlichen Divisor von $f(x)$ und $F(V_0, x)$ zu suchen und zwar die Operation so lange fortzusetzen, bis man zu einem Reste gelangt, der vom ersten Grade in x ist: Setzt man diesen Rest gleich Null, so erhält man eine Gleichung, welche den Werth von x_0

$$x_0 = \psi(V_0) \text{ oder } x_0 = \psi(V)$$

liefert, und dieser Werth von x_0 wird offenbar rational in V sein, da die Aufsuchung des grössten gemeinschaftlichen Divisors keine Wurzelgrösse einzuführen vermag.

Auf dieselbe Weise bestimmt man die übrigen Wurzeln, für welche sich gleichfalls rationale Ausdrücke, wie

$$x_0 = \psi_0(V), \; x_1 = \psi_1(V), \; \ldots, \; x_{n-1} = \psi_{n-1}(V)$$

ergeben.

Zusatz I. — Die Gleichung vom Grade $N = 1.2.3 \ldots n$ in V, welche alle N Werthe von V zu Wurzeln hat, und deren Coefficienten sich rational durch die Coefficienten der vorgelegten Gleichung ausdrücken lassen, besitzt die bemerkenswerthe Eigenschaft, dass alle ihre Wurzeln als rationale Functionen irgend einer von ihnen dargestellt werden können.

Es seien V und V_1 zwei Werthe von V; V_1 ist eine rationale Function der Wurzeln $x_0, x_1, \ldots, x_{n-1}$, welche nach dem Vorhergehenden rationale Functionen von V sind: man hat also

$$V_1 = \Theta(V),$$

und darin bezeichnet Θ eine rationale Function.

Zusatz II. — Wenn eine beliebige Anzahl algebraischer Irrationale gegeben ist, so können dieselben stets rational durch ein und dieselbe Irrationale ausgedrückt werden.

Unter einer algebraischen Irrationale verstehen wir jede Grösse, welche die Wurzel einer algebraischen Gleichung ist, deren Coefficienten rationale Functionen der als bekannt angesehenen Grössen sind. Dies vorausgesetzt, seien

$$x_0, x_1, \ldots, x_{m-1}$$

m beliebige algebraische Irrationale. Man kann eine Gleichung von einem gewissen Grade n mit kommensurabeln Coefficienten bilden, welche diese m Grössen zu Wurzeln hat, und welche keine wiederholten Wurzeln besitzt. Die n Wurzeln dieser Gleichung seien

$$x_0, x_1, \ldots, x_n,$$

und es bezeichne V eine rationale Function dieser Wurzeln, die in Folge der Substitutionen nur verschiedene Werthe annimmt. Dann ist V eine algebraische Irrationale, durch welche die m gegebenen Irrationalen nach dem vorhergehenden Lehrsatze rational ausgedrückt werden können.

Wir nehmen an, es sei unmittelbar einleuchtend, dass man stets eine rationale Function von m ungleichen Grössen bilden kann, die so beschaffen ist, dass die $1.2.3 \ldots m$ Werthe, die man daraus durch die Substitutionen herleitet, verschieden seien.

491. Anwendung auf ein Beispiel. — Der letzte Lehrsatz liefert eine Methode, die Wurzeln einer Gleichung zu bestim-

men, wenn man eine Function dieser Wurzeln kennt. Da diese Methode viel einfacher als diejenige ist, welche sich aus der Theorie von Lagrange ergiebt, so wollen wir sie an einem Beispiele kennen lernen. Wir betrachten die Gleichung dritten Grades.

$$(1). \qquad x^3 + p_1 x^2 + p_2 x + p_3 = 0$$

und setzen

$$V = a x_0 + b x_1 + c x_2.$$

Durch Transposition der Buchstaben x_1 und x_2 erhält man die beiden folgenden Werthe von V:

$$V_0 = a x_0 + b x_1 + c x_2,$$
$$V_1 = a x_0 + b x_2 + c x_1,$$

und die Gleichung in V ist

$$(V - V_0)(V - V_1) = 0,$$

oder

$$V^2 - [2 a x_0 + (b + c)(x_1 + x_2)] V$$
$$+ [a^2 x_0^2 + a(b+c) x_0 (x_1 + x_2) + bc(x_1^2 + x_2^2) + (b^2 + c^2) x_1 x_2] = 0.$$

Aus dieser Gleichung kann man x_1 und x_2 mittels der Relationen

$$x_1 + x_2 = -p_1 - x_0,$$
$$x_1 x_2 = p_2 - x_0(x_1 + x_2) = p_2 + p_1 x_0 + x_0^2,$$
$$x_1^2 + x_2^2 = (p_1^2 - 2 p_2) - x_0^2$$

entfernen und erhält

$$(2). \quad \left\{ \begin{array}{l} V^2 - [(2a - b - c) x_0 - p_1 (b + c)] V \\ \quad + [(a^2 + b^2 + c^2 - ab - ac - bc) x_0^2 \\ \quad + (b^2 + c^2 - ab - ac) p_1 x_0 + bc\, p_1^2 - (b-c)^2 p_2] = 0. \end{array} \right.$$

Um jetzt x_0 zu bestimmen, hat man im ersten Gliede der Gleichung (1) $x = x_0$ zu machen und den grössten gemeinschaftlichen Divisor des so erhaltenen Polynoms und des ersten Gliedes der Gleichung (2) zu suchen. In dem besonderen Falle, in welchem man

$$a^2 + b^2 + c^2 - ab - ac - bc = 0$$

hat, ist sogar überhaupt keine Rechnung erforderlich; denn die Gleichung (2) enthält dann nur noch die erste Potenz der Wurzel x_0 und lehrt deren Werth somit unmittelbar kennen. Dieser einfache Fall tritt ein, wenn man für a, b, c die drei kubischen Wurzeln der Einheit nimmt.

Es sei α eine complexe kubische Wurzel der Einheit, und es werde

$$a = 1 , b = \alpha , c = \alpha^2$$

gesetzt; dann ist, der Relation $\alpha^2 + \alpha + 1 = 0$ wegen,

$$x_0 = \frac{V^2 - p_1 V + (p_1^2 - 3 p_2)}{3 V} .$$

492. Eine Ergänzung des Lehrsatzes der No. 490 bildet der folgende Satz, der für die Theorie der Gleichungen von ebenso grosser Bedeutung ist.

Lehrsatz. — Es seien

(1). $$f(x) = 0$$

eine Gleichung n^{ten} Grades mit den n ungleichen Wurzeln $x_0 , x_1 , \ldots , x_{n-1}$, und

(2). $$V = \varphi(x_0 , x_1 , \ldots , x_{n-1})$$

eine rationale Function dieser Wurzeln und der bekannten Grössen, die so gewählt ist, dass die

$$N = 1 . 2 . 3 \ldots n$$

Functionen, welche daraus durch die Substitutionen der Wurzeln hergeleitet werden, numerisch ungleiche Werthe haben. Ferner seien

(3). $$\mathfrak{F}(V) = 0$$

die Gleichung N^{ten} Grades, welche die N Werthe von V zu Wurzeln hat, und $F(V)$ ein irreductibeler Divisor ν^{ten} Grades des Polynoms $\mathfrak{F}(V)$. Endlich mögen die Wurzeln der Gleichung

(4). $$F(V) = 0$$

mit

(5). $$V_0 , V_1 , V_2 , \ldots , V_{\nu-1}$$

bezeichnet werden. Wenn die Wurzeln der vorgelegten Gleichung (1) durch

(6). $$\psi_0(V_0) , \psi_1(V_0) , \ldots , \psi_{n-1}(V_0)$$

dargestellt werden, so kann man dieselben auch durch

(7). $$\psi_0(V_i) , \psi_1(V_i) , \ldots , \psi_{n-1}(V_i)$$

darstellen, wo V_i irgend eine der Grössen (5) bezeichnet.

Die Gleichung (1) besitzt der Voraussetzung nach die Wur-

zel $\psi_k(V_0)$; man hat daher $f\psi_k(V_0) = 0$, und folglich ist V_0 eine Wurzel der Gleichung

$$f\psi_k(V) = 0.$$

Nun ist V_0 eine der Wurzeln der Gleichung (4), und da diese Gleichung irreductibel ist, so müssen alle ihre Wurzeln der vorhergehenden Gleichung genügen. Man hat mithin $f\psi_k(V_i) = 0$, und dies drückt aus, dass die Grössen (7) Wurzeln der Gleichung (1) sind.

Um den Beweis des Satzes zu vollenden, hat man noch darzuthun, dass die Grössen (7) verschieden sind. Wir behaupten, es könne nicht $\psi_k(V_i) = \psi_j(V_i)$ sein, wofern nicht $k = j$ ist. Hätte man nämlich $\psi_k(V_i) = \psi_j(V_i)$, so würde V_i eine Wurzel der Gleichung

$$\psi_k(V) - \psi_j(V) = 0$$

sein, und letztere müsste alle Wurzeln (5) der irreductibelen Gleichung (4) zulassen. Man hätte also im Besondern

$$\psi_k(V_0) - \psi_j(V_0) = 0,$$

was der Voraussetzung widerspricht.

Zusatz. — Die Substitutionen $1, S_1, S_2, \ldots, S_{\nu-1}$, durch welche man von der Permutation (6) der Wurzeln $x_0, x_1, \ldots, x_{n-1}$ zu den ν Permutationen (7) übergeht, bilden ein conjugirtes System. Mit andern Worten: die ν Permutationen (7) machen eine Gruppe aus.

Man hat nämlich $V_i = \vartheta(V_0)$, wo ϑ eine rationale Function ist. Daraus geht hervor, dass V_0 eine Wurzel von $F\vartheta(V) = 0$ ist; diese Gleichung lässt daher die Wurzel V_j zu, und $\vartheta(V_j)$ ist eine der Wurzeln V_k der Gleichung (4). Bezeichnen wir, dies vorausgesetzt, die Permutation (7) mit A_i, so hat man

$$S_i A_0 = A_i = \psi_0\vartheta(V_0), \ \psi_1\vartheta(V_0), \ldots, \psi_{n-1}\vartheta(V_0),$$

und nach Ausführung der Substitution S_j

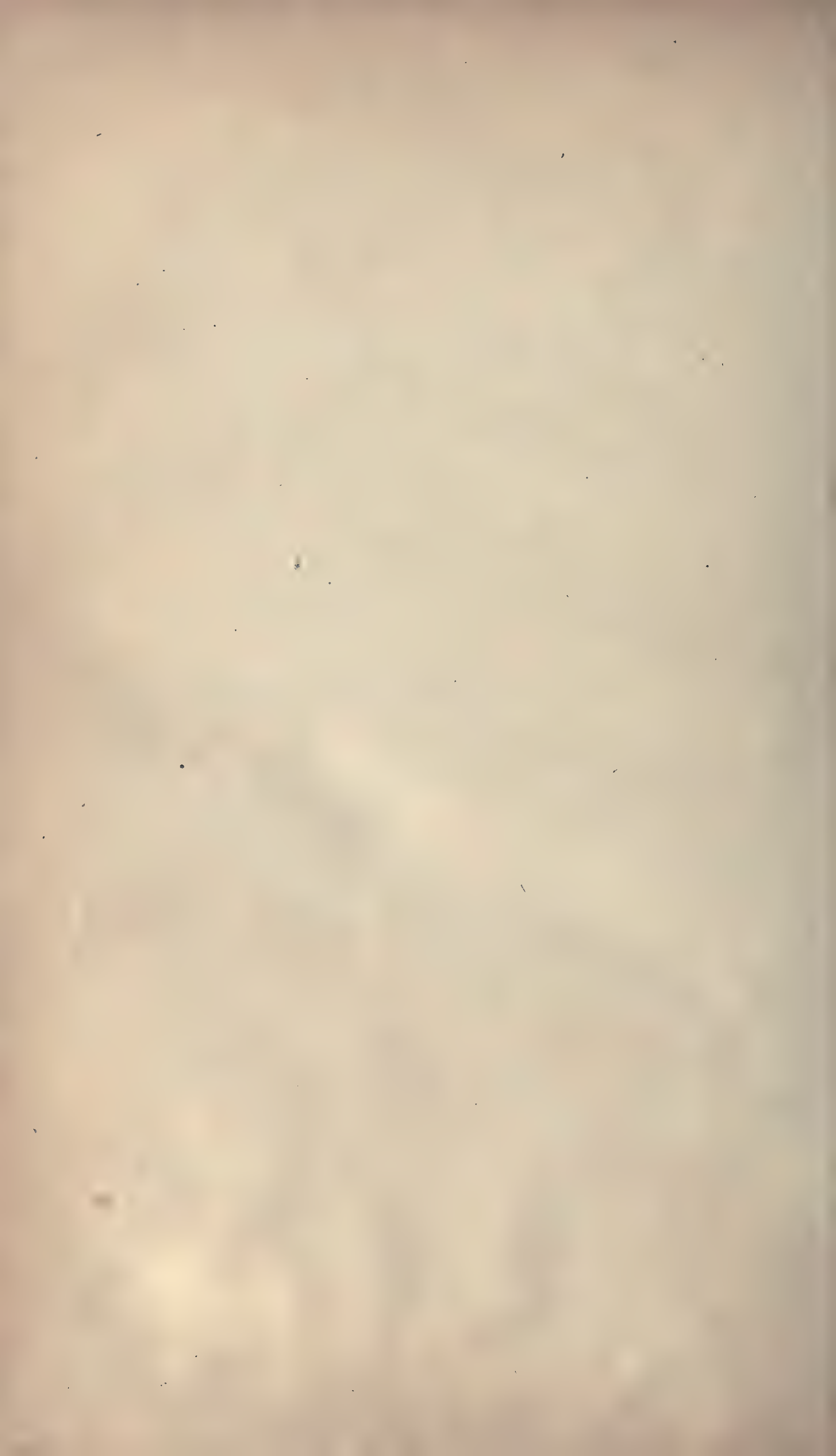
$$S_j S_i A_0 = \psi_0\vartheta(V_j), \psi_1\vartheta(V_j), \ldots, \psi_{n-1}\vartheta(V_j)$$
$$= \psi_0(V_k), \psi_1(V_k), \ldots, \psi_{n-1}(V_k),$$

mithin

$$S_j S_i = S_k.$$

Fünfter Theil.

Die algebraische Auflösung der Gleichungen.



Erstes Kapitel.

Gleichungen dritten und vierten Grades. Allgemeine Betrachtungen über die algebraische Auflösung der Gleichungen.

Auflösung der allgemeinen Gleichung dritten Grades.

493. Methode von Hudde. — Die einfachste aller Methoden, die man für die Auflösung der allgemeinen Gleichung dritten Grades kennt, ist jedenfalls die von Hudde. Diese Methode wollen wir daher auch zuerst darlegen.

Da man den zweiten Term einer Gleichung stets beseitigen kann, so werden wir die Gleichung

$$(1). \qquad x^3 + px + q = 0$$

betrachten, in welcher der Term in x^2 nicht mehr vorkommt. Wir setzen

$$(2). \qquad x = y + z,$$

wo y eine neue Veränderliche und z eine Function von y bezeichnet, über die wir so verfügen werden, dass die mittels der Relation (2) transformirte Gleichung wo möglich zu einer der Klassen von Gleichungen gehöre, die wir bereits zu lösen wissen. Ersetzt man in der Gleichung (1) x durch seinen aus (2) entnommenen Werth, so folgt

$$(y + z)^3 + p(y + z) + q = 0,$$

oder

$$(3). \qquad (y^3 + z^3 + q) + (y + z)(3yz + p) = 0.$$

Wird jetzt z durch die Bedingung

$$3yz + p = 0$$

bestimmt, welche

$$z = -\frac{p}{3y}$$

liefert, so geht die Gleichung (3) über in

$$y^3 - \frac{p^3}{27y^3} + q = 0,$$

oder in

$$(4).\qquad y^6 + qy^3 - \frac{p^3}{27} = 0.$$

Diese Gleichung in y kann nach Art der Gleichungen zweiten Grades gelöst werden, da sie nur die Potenzen y^3 und y^6 enthält. Hat man dann y bestimmt, so erhält man x durch die Formel

$$(5).\qquad x = y - \frac{p}{3y}.$$

Die Gleichung sechsten Grades (4), auf welche wir so die vorgelegte Gleichung zurückführen, hat von **Lagrange** den Namen: **Resolvente** der Gleichung (1) erhalten.

Obgleich diese Resolvente sechs Wurzeln besitzt, so liefert die Formel (5) doch nur drei Werthe von x, wie dies auch der Fall sein muss. Die Resolvente ändert sich nämlich nicht, wenn man y in $-\frac{p}{3y}$ verwandelt. Ihre sechs Wurzeln bilden daher drei Gruppen von der Beschaffenheit, dass das Produkt der beiden Wurzeln jeder Gruppe gleich $-\frac{p}{3}$ ist, und es liegt auf der Hand, dass die Formel (5) denselben Werth von x liefert, wenn man y der Reihe nach durch die beiden Wurzeln ein und derselben Gruppe ersetzt. Zum Ueberfluss wird sich dies auch noch aus dem Ausdrucke der Werthe von x ergeben, mit dem wir uns jetzt beschäftigen wollen.

Aus der Gleichung (4) folgt

$$y^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

oder, wenn der Kürze wegen

$$R = \frac{q^2}{4} + \frac{p^3}{27}$$

gesetzt wird,

$$(6).\qquad y^3 = -\frac{q}{2} \pm \sqrt{R};$$

aus der Gleichung (6) ergiebt sich endlich

(7). $$y = \sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}.$$

Der Vieldeutigkeit der Wurzelgrössen wegen liefert uns dieser Ausdruck die sechs Wurzeln der Gleichung (4). Wir setzen aber für die Folge fest, dass

$$\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}$$

nur eine der drei kubischen Wurzeln von $-\frac{q}{2} \pm \sqrt{R}$ darstelle; welche Wurzel dies sei, ist gleichgiltig; es muss jedoch immer dieselbe sein, so dass, wenn α und β die beiden complexen kubischen Wurzeln der Einheit bezeichnen, die sechs Wurzeln der Gleichung (4) in folgender Weise dargestellt werden können:

(8). $$\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}, \quad \alpha \sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}, \quad \beta \sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}.$$

Da nun die erste der beiden Wurzelgrössen

$$\sqrt[3]{-\frac{q}{2} + \sqrt{R}}, \quad \sqrt[3]{-\frac{q}{2} - \sqrt{R}}$$

nach dem Obigen diejenige der drei kubischen Wurzeln von

$$-\frac{q}{2} + \sqrt{R}$$

darstellt, welche wir wollen, und ebenso die zweite diejenige der drei kubischen Wurzeln von

$$-\frac{q}{2} - \sqrt{R},$$

welche wir wollen, und da ausserdem der Kubus ihres Produktes gleich $-\frac{p^3}{27}$ ist, so können wir die Werthe dieser Wurzelgrössen so wählen, dass ihr Produkt gleich $-\frac{p}{3}$ sei; dann hat man

(9). $$\sqrt[3]{-\frac{q}{2} \mp \sqrt{R}} = \frac{-p}{3\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}}.$$

Setzt man jetzt jeden der Werthe (8) von y in die Formel (5) ein, so erhält man mit Benutzung der Formel (9) und mit Rücksicht auf die bekannte Relation $\alpha\beta = 1$ die folgenden Werthe von x:

$$\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}} + \sqrt[3]{-\frac{q}{2} \mp \sqrt{R}},$$

$$\alpha\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}} + \beta\sqrt[3]{-\frac{q}{2} \mp \sqrt{R}},$$

$$\beta\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}} + \alpha\sqrt[3]{-\frac{q}{2} \mp \sqrt{R}},$$

welche sich augenscheinlich auf drei verschiedene Werthe reduciren, nämlich auf:

$$\sqrt[3]{-\frac{q}{2} + \sqrt{R}} + \sqrt[3]{-\frac{q}{2} - \sqrt{R}},$$

$$\alpha\sqrt[3]{-\frac{q}{2} + \sqrt{R}} + \beta\sqrt[3]{-\frac{q}{2} - \sqrt{R}},$$

$$\beta\sqrt[3]{-\frac{q}{2} + \sqrt{R}} + \alpha\sqrt[3]{-\frac{q}{2} - \sqrt{R}}.$$

Diese drei Wurzeln der Gleichung (1) können durch die eine Formel

$$(10). \qquad x = \sqrt[3]{-\frac{q}{2} + \sqrt{R}} + \sqrt[3]{-\frac{q}{2} - \sqrt{R}}$$

dargestellt werden, vorausgesetzt dass man den kubischen Wurzeln ihre volle Allgemeinheit lässt, aber nur die Werthe dieser Wurzelgrössen verbindet, deren Produkt gleich $-\frac{p}{3}$ ist. Die Formel (10) heisst die Cardanische Formel.

Wenn man in (10) jeden Werth der ersten kubischen Wurzel mit jedem Werthe der zweiten verbindet, so erhält man im Ganzen neun Werthe von x, welche die Wurzeln der folgenden drei Gleichungen sind:

$$x^3 + px + q = 0,$$
$$x^3 + p\alpha x + q = 0,$$
$$x^3 + p\beta x + q = 0;$$

hiervon überzeugt man sich leicht, wenn man aus der Gleichung (10) die Wurzelzeichen fortschafft.

494. Die vorstehende Untersuchung bezieht sich auf alle Fälle, die Grössen p und q mögen reell oder complex sein. Wir wollen den Fall, in welchem die Coefficienten reell sind, etwas näher in's Auge fassen.

Discussion der Cardanischen Formel. — p und q sind reelle Grössen. Wir setzen zunächst $R > 0$ oder

$$4p^3 + 27q^2 > 0$$

voraus; dann ist einer der drei Werthe jeder der beiden in (10) enthaltenen Wurzelgrössen reell. Bezeichnet A den reellen Werth der ersten, B denjenigen der zweiten, so hat die erste Wurzelgrösse die drei Werthe

$$A\ ,\ A\alpha\ ,\ A\beta\ ,$$

die zweite

$$B\ ,\ B\alpha\ ,\ B\beta\ .$$

Da nun die Werthe der beiden Wurzelgrössen, die man zu verbinden hat, ein reelles Produkt liefern müssen, so ergeben sich als die Wurzeln der Gleichung (1) die Grössen:

$$A + B,$$
$$A\alpha + B\beta,$$
$$A\beta + B\alpha.$$

Ausserdem ist

$$\alpha = \frac{-1+\sqrt{-3}}{2}\ ,\ \beta = \frac{-1-\sqrt{-3}}{2}\ ;$$

die drei Wurzeln der Gleichung (1) sind daher:

$$A + B\ ,\ -\frac{A+B}{2} \pm \frac{A-B}{2}\sqrt{-3}.$$

In diesem Falle hat also die Gleichung (1) zwei complexe Wurzeln.

Ist ferner $R = 0$ oder

$$4p^3 + 27q^2 = 0,$$

so ergiebt sich $B = A$; dann sind die drei Wurzeln von (1) sämmtlich reell, aber zwei derselben sind einander gleich.

Endlich setzen wir voraus, es sei $R < 0$ oder

$$4p^3 + 27q^2 < 0;$$

dann hat jede der beiden im Werthe von x vorkommenden Wurzelgrössen drei complexe Werthe, während man leicht erkennt, dass die Wurzeln der Gleichung (1) reell und ungleich sind. Sind nämlich

$$A + B\sqrt{-1}\ ,\ \alpha\,(A + B\sqrt{-1})\ ,\ \beta\,(A + B\sqrt{-1})$$

die drei kubischen Wurzeln des complexen Ausdrucks

$$-\frac{q}{2} + \sqrt{R}\,,$$

so hat der conjugirte complexe Ausdruck $-\frac{q}{2}-\sqrt{R}$ offenbar die kubischen Wurzeln

$$A-B\sqrt{-1}\ ,\ \beta(A-B\sqrt{-1})\ ,\ \alpha(A-B\sqrt{-1}),$$

und da die Werthe der beiden Wurzelgrössen, welche den Werth (10) von x bilden, ein reelles Produkt haben müssen, so erhält man die folgenden drei Werthe von x:

$$(A+B\sqrt{-1})+(A-B\sqrt{-1}),$$
$$\alpha(A+B\sqrt{-1})+\beta(A-B\sqrt{-1}),$$
$$\beta(A+B\sqrt{-1})+\alpha(A-B\sqrt{-1}),$$

oder, wenn α und β durch ihre Werthe ersetzt werden,

$$2A\ ,\ -A+B\sqrt{3}\ ,\ -A-B\sqrt{3}.$$

Die Wurzeln der Gleichung (1) sind daher in der That reell, und es ist leicht zu zeigen, dass sie auch ungleich sind.

Erstens kann nämlich nicht

$$-A+B\sqrt{3}=-A-B\sqrt{3}$$

sein; denn daraus würde $B=0$ folgen, und $-\frac{q}{2}+\sqrt{R}$ würde der Voraussetzung zuwider gleich der reellen Grösse A^3 sein.

Ferner kann aber auch nicht

$$2A=-A\pm B\sqrt{3}$$

sein; denn daraus würde sich $B=\pm A\sqrt{3}$ ergeben; es wäre folglich

$$A+B\sqrt{-1}=A(1\pm\sqrt{-3})=-2\alpha A,$$

und

$$-\frac{q}{2}+\sqrt{R}=-8\alpha^3A^3=-8A^3.$$

Auch diese Gleichung widerspricht der Voraussetzung, da ihr zweites Glied reell ist.

Der Fall, den wir hier untersuchen, ist sehr bemerkenswerth; denn obgleich die drei Wurzeln der Gleichung dritten Grades reell sind, so stellt die Cardanische Formel ihre Werthe doch unter einer mit complexen Grössen behafteten Form dar; und wollte man, um diese complexen Grössen fortzuschaffen, die kubischen Wurzeln, welche in die Cardanische Formel eingehen, auf die Form $A+B\sqrt{-1}$ bringen, so würde man finden, dass die Grössen A und B von einer der vorgelegten ganz ähnlichen Gleichung

abhängen. Die Wurzeln der Gleichung in A z. B. würden reell sein, so dass in dem Ausdrucke von A gleichfalls complexe Grössen vorkämen. Aus diesem Grunde hat man den vorliegenden Fall irreductibel („casus irreductibilis") genannt.

495. Nach dem Vorhergehenden kann die Cardanische Formel zur numerischen Auflösung der Gleichung dritten Grades nur dann benutzt werden, wenn eine, aber auch nur eine der drei Wurzeln reell ist. Im irreductibelen Falle führt die Anwendung von Kreisfunctionen leicht zum Ziele. Setzt man nämlich

$$\frac{q^2}{4} + \frac{p^3}{27} = -\varrho^2 \sin^2 \omega, \; -\frac{q}{2} = \varrho \cos \omega,$$

so sind ϱ und ω durch die Formeln

$$\varrho = \sqrt{\frac{-p^3}{27}}\,, \; \cos \omega = \frac{\frac{-q}{2}}{\sqrt{\frac{-p^3}{27}}}$$

bestimmt, und die Cardanische Formel liefert

$$x = \sqrt[3]{\varrho}\left(\sqrt[3]{\cos \omega + \sqrt{-1}\sin \omega} + \sqrt[3]{\cos \omega - \sqrt{-1}\sin \omega}\right),$$

wo $\sqrt[3]{\varrho}$ eine reelle Grösse bezeichnet. Ausserdem hat man

$$\sqrt[3]{\cos \omega - \sqrt{-1}\sin \omega} = \cos\frac{\omega + 2k\pi}{3} - \sqrt{-1}\sin\frac{\omega + 2k\pi}{3},$$

$$\sqrt[3]{\cos \omega + \sqrt{-1}\sin \omega} = \cos\frac{\omega + 2k\pi}{3} + \sqrt{-1}\sin\frac{\omega + 2k\pi}{3},$$

wo k einen der drei Werthe 0, 1, 2 hat. In diesen beiden Formeln muss man k denselben Werth ertheilen, da das Produkt ihrer beiden ersten Glieder reell sein soll; man hat daher

$$x = 2\sqrt[3]{\varrho}\cos\frac{\omega + 2k\pi}{3},$$

und die drei Wurzeln der Gleichung sind

$$2\sqrt[3]{\varrho}\cos\frac{\omega}{3}, \; 2\sqrt[3]{\varrho}\cos\frac{\omega + 2\pi}{3}, \; 2\sqrt[3]{\varrho}\cos\frac{\omega + 4\pi}{3}.$$

Die Werthe dieser Wurzeln lassen sich in jedem Falle mit Hülfe der Logarithmen berechnen.

496. Methode von Lagrange. — Wir betrachten die vollständige Gleichung dritten Grades

$$(1). \qquad x^3 + Px^2 + Qx + R = 0$$

und bezeichnen ihre drei Wurzeln mit x_0, x_1, x_2. Der in No. 489 u. No. 490 dargelegten Theorie zufolge kann man x_0, x_1, x_2 be-

stimmen, wenn es gelingt, den Werth irgend einer Function dieser Wurzeln zu ermitteln, die indess so gewählt sein muss, dass die sechs Werthe, welche sie durch die 1 . 2 . 3 Substitutionen von x_0, x_1, x_2 annehmen kann, von einander verschieden seien. Die Methode von Lagrange, die wir jetzt kennen lernen wollen, besteht darin, den Werth einer linearen Function der drei Wurzeln, wie

$$t = x_0 + Ax_1 + Bx_2, \tag{2}$$

in welcher A, B irgendwelche Constanten bezeichnen, direkt zu bestimmen, und aus dieser Function sodann den Ausdruck der Wurzeln selbst herzuleiten.

Vollzieht man an den Indices 0, 1, 2 alle Substitutionen, welche sie gestatten, so erhält man die folgenden sechs Werthe der Function t:

$$(3).\quad \begin{cases} t_0 = x_0 + Ax_1 + Bx_2, \\ t_1 = x_0 + Ax_2 + Bx_1, \\ t_2 = x_1 + Ax_2 + Bx_0, \\ t_3 = x_1 + Ax_0 + Bx_2, \\ t_4 = x_2 + Ax_0 + Bx_1, \\ t_5 = x_2 + Ax_1 + Bx_0, \end{cases}$$

und t hängt von der Gleichung 6ten Grades

$$(t - t_0)(t - t_1)(t - t_2)(t - t_3)(t - t_4)(t - t_5) = 0 \tag{4}$$

ab, die man auf eine Gleichung zweiten Grades zurückführen kann, wenn sich über die unbestimmten Constanten A und B so verfügen lässt, dass (4) nur die sechste und die dritte Potenz von t enthält. Damit dies der Fall sei, ist erforderlich und hinreichend, dass, wenn t irgend eine der Wurzeln von (4) und α eine complexe kubische Wurzel der Einheit bezeichnen, auch αt und $\alpha^2 t$ Wurzeln von (4) seien. Sehen wir, ob diese Bedingung erfüllt werden kann. Zunächst können αt_0 und $\alpha^2 t_0$ weder gleich t_1, noch gleich t_3, noch gleich t_5 sein, wenn man x_0, x_1, x_2 als unbestimmte Grössen ansieht; denn sonst hätte man $\alpha = 1$. Es muss daher entweder

$$\alpha t_0 = t_2 \text{ und } \alpha^2 t_0 = t_4,$$

oder

$$\alpha t_0 = t_4 \text{ und } \alpha^2 t_0 = t_2$$

sein. Die beiden letzten Gleichungen sind den ersteren äquivalent, da die Wurzeln α und α^2 sich durch Nichts von einander unter-

scheiden. Wir werden die beiden letzten Gleichungen annehmen, und da dieselben für alle Werthe von x_0, x_1, x_2 stattfinden müssen, so ergeben sich folgende Werthe von A und B:

$$A = \alpha \ , \ B = \alpha^2.$$

Wenn A und B diese Werthe haben, so ist auch

$$\alpha t_1 = t_3 \ , \ \alpha^2 t_1 = t_5.$$

Nimmt man daher

$$t = x_0 + \alpha x_1 + \alpha^2 x_2$$

an, so hat die Gleichung in t die Wurzeln

$$t_0 \ , \ \alpha t_0 \ , \ \alpha^2 t_0 \ , \ t_1 \ , \ \alpha t_1 \ , \ \alpha^2 t_1.$$

Diese Gleichung ist folglich

$$(t^3 - t_0^3)\,(t^3 - t_1^3) = 0,$$

oder

$$(5). \qquad t^6 - (t_0^3 + t_1^3)\, t^3 + t_0^3 t_1^3 = 0,$$

wenn

$$(6). \qquad \begin{cases} t_0 = x_0 + \alpha x_1 + \alpha^2 x_2, \\ t_1 = x_0 + \alpha^2 x_1 + \alpha x_2 \end{cases}$$

gemacht wird. Dies stimmt mit den allgemeinen Resultaten überein, die wir in No. 482 erhalten haben.

Kennt man die Werthe von t_0 und t_1, so macht die Bestimmung von x_0, x_1, x_2 keine Schwierigkeit mehr. Es ist nämlich

$$(7). \qquad -P = x_0 + x_1 + x_2,$$

und durch Addition der Gleichungen (6) und (7) ergiebt sich der Relation $\alpha^2 + \alpha + 1 = 0$ wegen

$$(8). \qquad x_0 = \frac{-P + t_0 + t_1}{3}.$$

Um x_1 zu bestimmen, hat man die drei Gleichungen (6) und (7) zu addiren, nachdem dieselben beziehungsweise mit α^2, α, 1 multiplicirt sind; man erhält

$$(9). \qquad x_1 = \frac{-P + \alpha^2 t_0 + \alpha t_1}{3}.$$

Endlich ergiebt sich noch

$$(10). \qquad x_2 = \frac{-P + \alpha t_0 + \alpha^2 t_1}{3},$$

wenn man die Gleichungen (6) und (7) beziehungsweise mit α, α^2, 1 multiplicirt und sodann addirt.

Es ist somit Alles darauf zurückgeführt, die Gleichung (5)

aufzulösen, welche deshalb eine **Resolvente** der vorgelegten Gleichung ist. Wir wollen zunächst die Coefficienten der Resolvente durch diejenigen der vorgelegten Gleichung ausdrücken, was deshalb möglich ist, weil diese Coefficienten $t_0^3 + t_1^3$, $t_0^3 t_1^3$ symmetrische Functionen der Wurzeln sind.

Durch Multiplication der beiden Gleichungen (6) ergiebt sich mit Rücksicht auf die Relation $\alpha^2 + \alpha + 1 = 0$

$$t_0 t_1 = x_0^2 + x_1^2 + x_2^2 - x_0 x_1 - x_1 x_2 - x_2 x_0$$
$$= (x_0 + x_1 + x_2)^2 - 3(x_0 x_1 + x_1 x_2 + x_2 x_0),$$

folglich

$$(11). \qquad t_0 t_1 = P^2 - 3Q.$$

Erhebt man endlich jede der Gleichungen (6) auf die dritte Potenz und addirt die Resultate, so folgt

$$t_0^3 + t_1^3 = 2(x_0^3 + x_1^3 + x_2^3)$$
$$- 3(x_0^2 x_1 + x_1^2 x_0 + x_1^2 x_2 + x_2^2 x_1 + x_2^2 x_0 + x_0^2 x_2) + 12 x_0 x_1 x_2$$
$$= 3(x_0^3 + x_1^3 + x_2^3) - (x_0 + x_1 + x_2)^3 + 18 x_0 x_1 x_2$$
$$= -2P^3 + 9PQ - 27R.$$

Die Resolvente (5) ist daher

$$t^6 - (-2P^3 + 9PQ - 27R)\, t^3 + (P^2 - 3Q)^3 = 0,$$

und sie reducirt sich, wenn

$$t^3 = \vartheta$$

gesetzt wird, auf die Gleichung zweiten Grades

$$\vartheta^2 - (-2P^3 + 9PQ - 27R)\, \vartheta + (P^2 - 3Q)^3 = 0.$$

Bezeichnet man die beiden Wurzeln der letzteren mit ϑ_0 und ϑ_1, so hat man

$$t_0 = \sqrt[3]{\vartheta_0}\,,\; t_1 = \sqrt[3]{\vartheta_1}\,,$$

und die Gleichungen (8), (9) und (10) gehen über in

$$x_0 = \frac{-P + \sqrt[3]{\vartheta_0} + \sqrt[3]{\vartheta_1}}{3},$$

$$x_1 = \frac{-P + \alpha^2 \sqrt[3]{\vartheta_0} + \alpha \sqrt[3]{\vartheta_1}}{3},$$

$$x_2 = \frac{-P + \alpha \sqrt[3]{\vartheta_0} + \alpha^2 \sqrt[3]{\vartheta_1}}{3}.$$

Für $\sqrt[3]{\vartheta_0}$ hat man irgend einen der drei Werthe dieser Wurzelgrösse, aber in allen drei Formeln denselben Werth zu nehmen.

Sobald man für $\sqrt[3]{\vartheta_0}$ einen bestimmten Werth angenommen hat, ist der Werth von $\sqrt[3]{\vartheta_1}$ nicht mehr willkürlich, da die Gleichung (11)

$$\sqrt[3]{\vartheta_0}\,\sqrt[3]{\vartheta_1} = P^2 - 3Q$$

liefert. Daraus geht hervor, dass die drei Wurzeln durch die eine Formel

$$x = \frac{-P + \sqrt[3]{\vartheta_0} + \sqrt[3]{\vartheta_1}}{3}$$

dargestellt werden können, welche nur drei verschiedene Werthe enthält, wenn man bedenkt, dass $\sqrt[3]{\vartheta_1}$ der Kürze wegen statt $\dfrac{P^2 - 3Q}{\sqrt[3]{\vartheta_0}}$ gesetzt ist.

497. Vergleichung der beiden vorhergehenden Methoden. — Die im Vorhergehenden betrachtete Methode von Lagrange ist zwar nicht so einfach, dafür aber direkter als diejenige von Hudde. Beide Methoden liefern jedoch dieselbe Resultante, und wir wollen jetzt zeigen, dass man durch tieferes Eingehen in die Methode von Hudde naturgemäss zu derjenigen von Lagrange geführt wird.

Wir nehmen wieder die allgemeine Gleichung dritten Grades

$$(1).\qquad x^3 + Px^2 + Qx + R = 0$$

auf. Um die Methode von Hudde anzuwenden, hat man zunächst den zweiten Term zu beseitigen, indem man

$$x = -\frac{P}{3} + x'$$

setzt, wodurch die Gleichung auf die Form

$$(2).\qquad x'^3 + px' + q = 0$$

gebracht wird. Darauf setzt man

$$x' = y - \frac{p}{3y},$$

und erhält endlich die Resolvente

$$(3).\qquad y^6 + qy^3 - \frac{p^3}{27} = 0.$$

Bezeichnet nun y_0 eine der drei kubischen Wurzeln von

$$-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

und y_1 diejenige der drei kubischen Wurzeln von

$$-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^6}{27}},$$

welche mit y_0 multiplicirt das Produkt $\frac{-p}{3}$ liefert, so hat die Gleichung (3) die Wurzeln

$$y_0\,,\ \alpha y_0\,,\ \alpha^2 y_0\,,\ y_1\,,\ \alpha y_1\,,\ \alpha^2 y_1\,,$$

und die Wurzeln von (2) sind

$$y_0+y_1\,,\ \alpha y_0+\alpha^2 y_1\,,\ \alpha^2 y_0+\alpha y_1.$$

Werden also die drei Wurzeln der Gleichung (1) mit x_0, x_1, x_2 bezeichnet, so erhält man

$$x_0=-\frac{P}{3}+y_0+y_1,$$

$$x_1=-\frac{P}{3}+\alpha^2 y_0+\alpha y_1,$$

$$x_2=-\frac{P}{3}+\alpha y_0+\alpha^2 y_1.$$

Addirt man diese Gleichungen, nachdem man sie zuerst beziehungsweise mit $1, \alpha, \alpha^2$, dann beziehungsweise mit $1, \alpha^2, \alpha$ multiplicirt hat, so folgt

$$y_0=\frac{x_0+\alpha x_1+\alpha^2 x_2}{3},$$

$$y_1=\frac{x_0+\alpha^2 x_1+\alpha x_2}{3}.$$

Daraus ist ersichtlich, dass die Methode von Hudde im Grunde darauf hinausläuft, eine Resolvente in y zu bilden, deren Wurzel den Werth

$$y=\frac{x_0+\alpha x_1+\alpha^2 x_2}{3}$$

hat, und dass diese Resolvente sich nur durch den Factor 3, durch welchen die Wurzeln dividirt werden, von der Resolvente von Lagrange unterscheidet.

498. Methoden von Tschirnaus und von Euler. — Wir haben in No. 190 die allgemeine Methode von Tschirnaus kennen gelernt, mittels welcher beliebig viele Terme einer Gleichung zum Verschwinden gebracht werden. Es ergiebt sich daraus eine Methode für die Auflösung der Gleichungen dritten Grades. Wir werden hier aber den in No. 191 über diesen Gegenstand gemachten Bemerkungen Nichts mehr hinzufügen.

Die Methode von Euler unterscheidet sich nur der Form nach von derjenigen von Tschirnaus. Sie besteht darin, y aus zwei Gleichungen von der Form

$$ay^2 + by + c = x \ , \ y^3 = d$$

zu eliminiren und die Endgleichung in x identisch gleich der vorgelegten Gleichung zu setzen; dann ergiebt sich offenbar die Auflösung der letzteren. Ueber den Werth einer der unbestimmten Grössen a, b, c, d kann man nach Belieben verfügen; man kann z. B. $a = 1$ oder $d = 1$ machen.

Ueber die Gleichungen dritten Grades, bei denen zwei Wurzeln rational durch die dritte Wurzel und durch die bekannten Grössen ausgedrückt werden können.

499. Wenn man mit x, x_1, x_2 die Wurzeln der Gleichung dritten Grades

$$(1). \qquad x^3 + Px^2 + Qx + R = 0$$

bezeichnet, so hat das Produkt der quadrirten Wurzeldifferenzen

$$\Delta = (x - x_1)^2 (x - x_2)^2 (x_1 - x_2)^2$$

nach No. 179 den Werth

$$\Delta = -(4Q^3 + 27R^2) + 18PQR + P^2Q^2 - 4P^3R.$$

Multiplicirt man, dies vorausgesetzt, die Identität

$$\sqrt{\Delta} = (x - x_1)(x - x_2)(x_2 - x_1)$$

mit $x_1 - x_2$, so ergiebt sich

$$(x_1 - x_2)\sqrt{\Delta} = [(x_1 - x)(x_1 - x_2)]\,[(x_2 - x)(x_2 - x_1)]$$

oder

$$\begin{aligned}(x_1 - x_2)\sqrt{\Delta} &= (3x_1^2 + 2Px_1 + Q)(3x_2^2 + 2Px_2 + Q) \\ &= 9x_1^2x_2^2 + 6Px_1x_2(x_1 + x_2) + 3Q(x_1 + x_2)^2 \\ &\quad + (4P^2 - 6Q)x_1x_2 + 2PQ(x_1 + x_2) + Q^2.\end{aligned}$$

Ausserdem hat man

$$(2). \qquad x_1 + x_2 = -x - P$$

und

$$x_1x_2 = -(x_1 + x_2)x + Q = x^2 + Px + Q.$$

Durch Benutzung dieser Formeln erhält man

$$\begin{aligned}(x_1 - x_2)\sqrt{\Delta} &= 9x^4 + 12Px^3 + (15Q + P^2)x^2 \\ &\quad + (10PQ - 2P^3)x + (4Q^2 - P^2Q).\end{aligned}$$

Mittels der Gleichung (1) lässt sich dieser Ausdruck auf den zweiten Grad in Beziehung auf x reduciren, nämlich auf

$$(3).\quad \begin{cases} (x_1 - x_2)\sqrt{\Delta} = (6Q - 2P^2)\,x^2 - (9R - 7PQ + 2P^3)\,x \\ \qquad + (4Q^2 - P^2Q - 3PR). \end{cases}$$

Aus den Gleichungen (2) und (3) ist ersichtlich, dass die Wurzeln x_1 und x_2 gleich den beiden Werthen von X sind, welche die Formel

$$(4).\quad \begin{cases} X = \frac{1}{2\sqrt{\Delta}}\,[(6Q - 2P^2)\,x^2 - (9R - 7PQ + 2P^3 + \sqrt{\Delta})\,x \\ \qquad + (4Q^2 - P^2Q - 3PR - P\sqrt{\Delta})] \end{cases}$$

liefert, wenn man darin der Wurzelgrösse $\sqrt{\Delta}$ der Reihe nach ihre beiden Werthe ertheilt.

Zählt man also $\sqrt{\Delta}$ zu den als bekannt angesehenen Grössen, so sind die Wurzeln x_1 und x_2 als rationale Functionen der Wurzel x und der bekannten Grössen ausgedrückt.

Man kann diese Wurzeln auch durch rationale und lineare Functionen von x darstellen, indem man den in No. 183 angegebenen Weg einschlägt. Dividirt man nämlich das erste Glied $F(x)$ der Gleichung (1) durch den Ausdruck (4) von X und bezeichnet den Quotienten dieser Division mit V, den Rest mit $-U$, so ist

$$0 = F(x) = VX - U,$$

folglich

$$X = \frac{U}{V}.$$

Durch Ausführung jener Division ergiebt sich

$$2\sqrt{\Delta}\,.\,V = (6Q - 2P^2)\,x + (9R - PQ + \sqrt{\Delta}),$$

$$2\sqrt{\Delta}\,.\,U = -(9R - PQ - \sqrt{\Delta})x + (2Q^2 - 6PR).$$

Setzt man daher

$$(5).\quad \begin{cases} a = \frac{\sqrt{\Delta} - (9R - PQ)}{2\sqrt{\Delta}}, \\ b = \frac{2Q^2 - 6PR}{2\sqrt{\Delta}}, \\ a' = \frac{6Q - 2P^2}{2\sqrt{\Delta}}, \\ b' = \frac{\sqrt{\Delta} + (9R - PQ)}{2\sqrt{\Delta}}, \end{cases}$$

so ist der Ausdruck von X:

$$X = \frac{ax + b}{a'x + b'},$$

und man erhält daraus die Wurzeln x_1 und x_2, wenn man der Wurzelgrösse $\sqrt{\Delta}$ ihre beiden Werthe ertheilt. Wenn man aber $\sqrt{\Delta}$ in $-\sqrt{\Delta}$ verwandelt, so geht a in b', b in $-b$, a' in $-a'$ und b' in a über; man kann daher

$$x_1 = \frac{ax+b}{a'x+b'}\ ,\ x_2 = \frac{b'x-b}{-a'x+a}$$

schreiben. Aus den Gleichungen (5) folgt

(6). $$a+b'=1\ ,\ ab'-ba'=1.$$

Setzt man also

(7). $$\vartheta x = \frac{ax+b}{a'x+b'},$$

so erhält man

(8). $$\vartheta^2 x = \frac{b'x-b}{-a'x+a}\ ,\ \vartheta^3 x = x;$$

darin ist $\vartheta^2 x$ statt $\vartheta\vartheta x$, $\vartheta^3 x$ statt $\vartheta\vartheta^2 x$ geschrieben.

Die Wurzeln der vorgelegten Gleichung können danach durch

$$x\ ,\ \vartheta x\ ,\ \vartheta^2 x$$

dargestellt werden. Wir fügen hinzu, dass, wenn eine lineare Function

$$\varphi(x) = \frac{\alpha x+\beta}{\alpha' x+\beta'},$$

deren Determinante $\alpha\beta'-\beta\alpha'$ immer gleich 1 vorausgesetzt werden kann, eine der Wurzeln, z. B. ϑx, darstellt, man identisch

$$\varphi(x) = \vartheta x,$$

d. h.

$$\alpha = \pm a\ ,\ \beta = \pm b\ ,\ \alpha' = \pm a'\ ,\ \beta' = \pm b'$$

hat. Da nämlich die vorgelegte Gleichung irreductibel ist, so kann sie keine Wurzel mit der Gleichung zweiten Grades $\varphi(x) = \vartheta x$ gemeinschaftlich haben, wofern letztere nicht identisch besteht.

500. In No. 166 haben wir eine Gleichung dritten Grades kennen gelernt, deren Wurzeln sich in Kettenbrüche entwickeln lassen, welche mit demselben vollständigen Quotienten schliessen. Die vorhergehende Untersuchung lehrt uns alle Gleichungen dritten Grades kennen, welche diese Eigenschaft besitzen. Damit nämlich zwei Irrationale x und x_1 in Kettenbrüche entwickelt werden können, welche in dieselben Quotienten auslaufen, ist nach No. 16 erforderlich und hinreichend, dass man

$$x_1 = \frac{ax+b}{a'x+b'}$$

habe, worin a, b, a', b' positive oder negative ganze Zahlen sind, welche der Bedingung

$$ab' - ba' = \pm 1$$

genügen.

Wendet man dieses Resultat auf zwei der Wurzeln der Gleichung (1), auf x und ϑx, oder auf x und $\vartheta^2 x$ an, so wird die hinsichtlich der Determinante gestellte Bedingung offenbar erfüllt, wenn man ϑx oder $\vartheta^2 x$ durch die Formeln (5), (7) und (8) ausdrückt. Damit also die Kettenbrüche, welche die drei Wurzeln darstellen, ein und denselben vollständigen Quotienten gemeinschaftlich haben, ist erforderlich und hinreichend, dass die Formeln (5) für a, b, a', b' ganze Werthe liefern.

Die beiden letzten Gleichungen (5) können durch die Gleichungen (6) ersetzt werden, und diese liefern

$$(9). \qquad b' = 1 - a\,, \quad b = -\frac{1 - a + a^2}{a'}.$$

Zugleich folgt aus den beiden ersten Gleichungen (5)

$$(10). \qquad 9R - PQ = (1 - 2a)\sqrt{\Delta},\ 3Q - P^2 = a'\sqrt{\Delta},$$

und der Ausdruck von Δ kann auf die Form

$$(11). \quad \left\{ \begin{aligned} 9\Delta = &- 3(9R - PQ)^2 + 4P(9R - PQ)(3Q - P^2) \\ &- 4Q(3Q - P^2)^2 \end{aligned} \right.$$

gebracht werden. Aus den Gleichungen (10) und (11) entnehmen wir:

$$(12). \quad \left\{ \begin{aligned} Q &= -\frac{3(1 - a + a^2)}{a'^2} + \frac{1 - 2a}{a'} P, \\ R &= \frac{(-1 + 2a)(1 - a + a^2)}{a'^3} + \frac{a(-1 + a)}{a'^2} P, \\ \sqrt{\Delta} &= \frac{3Q - P^2}{a'}; \end{aligned} \right.$$

die Grösse P bleibt unbestimmt.

Danach ist der allgemeine Ausdruck der Gleichungen, mit denen wir uns beschäftigen,

$$(13). \quad \left\{ \begin{aligned} &x^3 + Px^2 + \left[\frac{-3(1 - a + a^2)}{a'^2} + \frac{1 - 2a}{a'} P\right] x \\ &\qquad + \left[\frac{(-1 + 2a)(1 - a + a^2)}{a'^3} + \frac{a(-1 + a)}{a'^2} P\right] = 0. \end{aligned} \right.$$

Darin bezeichnet P irgend eine rationale oder irrationale reelle Grösse, a irgend eine positive oder negative ganze Zahl; a' end-

lich ist irgend ein positiver oder negativer Divisor der Zahl $1 - a + a^2$.

Die Gleichung

$$x^3 - 7x + 7 = 0,$$

die wir in No. 166 betrachtet haben, entspricht den Werthen

$$P = 0 \ , \ a = -4 \ , \ a' = -3.$$

Auflösung der allgemeinen Gleichung vierten Grades.

501. Methode von Ferrari. — Die älteste und zugleich einfachste Methode, die Gleichung vierten Grades aufzulösen, ist die von Ferrari. Sie besteht darin, beide Glieder der Gleichung in Quadrate zu verwandeln, und führt folglich die Auflösung dieser Gleichung auf die Auflösung zweier Gleichungen zweiten Grades zurück.

Lässt man nur die beiden ersten Terme der allgemeinen Gleichung vierten Grades

$$(1). \qquad x^4 + px^3 + qx^2 + rx + s = 0$$

im ersten Gliede stehen, so erhält man

$$x^4 + px^3 = -qx^2 - rx - s.$$

Um nun das erste Glied zu einem vollständigen Quadrate zu machen, addiren wir beiderseits $\frac{p^2x^2}{4}$; dann ergiebt sich:

$$(2). \qquad \left(x^2 + \frac{p}{2}x\right)^2 = \left(\frac{p^2}{4} - q\right)x^2 - rx - s.$$

In dieser Form würde sich die vorgelegte Gleichung sofort auflösen lassen, wenn das zweite Glied ein Quadrat wäre; denn dann würde man nur die zweite Wurzel aus beiden Gliedern zu ziehen haben, um zu einer Gleichung zweiten Grades zu gelangen. Auf diesen besonderen Fall führt die Methode von Ferrari alle übrigen Fälle zurück.

Bezeichnet man mit y eine unbestimmte Grösse und fügt beiden Gliedern der Gleichung (2)

$$\left(x^2 + \frac{p}{2}x\right)y + \frac{y^2}{4}$$

hinzu, so folgt

$$(3). \quad \left(x^2 + \frac{p}{2}x + \frac{y}{2}\right)^2 = \left(\frac{p^2}{4} - q + y\right)x^2 + \left(\frac{py}{2} - r\right)x + \left(\frac{y^2}{4} - s\right).$$

Jetzt bestimmen wir y in der Weise, dass das zweite Glied der Gleichung (3) ein Quadrat wird. Zu diesem Zwecke genügt es, dass man

$$\left(\frac{py}{2} - r\right)^2 = \left(\frac{p^2}{4} - q + y\right)(y^2 - 4s),$$

oder

$$(4).\quad y^3 - qy^2 + (pr - 4s)\,y - s\,(p^2 - 4q) - r^2 = 0$$

habe, und wenn man eine einzige Wurzel dieser Gleichung in y kennt, so ergiebt sich die Auflösung der vorgelegten Gleichung (1) auf der Stelle; denn die Gleichung (3), welche mit (1) übereinstimmt, kann folgendermassen geschrieben werden:

$$\left(x^2 + \frac{p}{2}x + \frac{y}{2}\right)^2 - \left(\frac{p^2}{4} - q + y\right)\left[x + \frac{p\,\frac{y}{2} - r}{2\left(\frac{p^2}{4} - q + y\right)}\right]^2 = 0,$$

und diese letztere Gleichung zerfällt in die beiden Gleichungen zweiten Grades:

$$(5).\quad \begin{cases} x^2 + \left(\frac{p}{2} + \sqrt{\frac{p^2}{4} - q + y}\right)x + \left[\frac{y}{2} + \frac{\frac{py}{2} - r}{2\sqrt{\frac{p^2}{4} - q + y}}\right] = 0, \\ x^2 + \left(\frac{p}{2} - \sqrt{\frac{p^2}{4} - q + y}\right)x + \left[\frac{y}{2} - \frac{\frac{py}{2} - r}{2\sqrt{\frac{p^2}{4} - q + y}}\right] = 0. \end{cases}$$

Die kubische Gleichung (4) ist somit die Resolvente der Gleichung (1). Nun haben wir gesehen, dass sich die Wurzeln der allgemeinen Gleichung dritten Grades algebraisch ausdrücken lassen. Dieselbe Eigenschaft hat folglich die Gleichung vierten Grades; denn die Gleichungen (5) liefern die vier Wurzeln der Gleichung (1), ausgedrückt durch die Coefficienten und irgendeine Wurzel y der Resolvente.

502. Betrachtung der Resolvente. — Wir haben soeben gesehen, dass die vier Wurzeln der vorgelegten Gleichung als Functionen einer einzigen Wurzel der Resolvente dargestellt werden können. Jetzt wollen wir diese Resolvente näher in's Auge fassen und untersuchen, auf welche Weise ihre Wurzeln aus denjenigen der vorgelegten Gleichung zusammengesetzt werden.

Wir bezeichnen wieder mit y irgend eine Wurzel der Resolvente und mit x_0, x_1, x_2, x_3 die vier Wurzeln der vorgelegten Gleichung, nämlich mit x_0 und x_2 die Wurzeln, welche der ersten, mit x_1 und x_3 diejenigen, welche der zweiten der Gleichungen (5) zukommen. Dann hat man

$$x_0 x_2 = \frac{y}{2} + \frac{\frac{py}{2} - r}{2\sqrt{\frac{p^2}{4} - q + y}},$$

$$x_1 x_3 = \frac{y}{2} - \frac{\frac{py}{2} - r}{2\sqrt{\frac{p^2}{4} - q + y}},$$

und daraus folgt

$$y = x_0 x_2 + x_1 x_3.$$

Die Resolvente hat daher die Function

$$x_0 x_2 + x_1 x_3$$

der vier Wurzeln der vorgelegten Gleichung zur Wurzel, und diese Function nimmt in der That durch die Substitutionen der Wurzeln nur drei verschiedene Werthe an.

Setzen wir

$$t = 2\sqrt{\frac{p^2}{4} - q + y},$$

also

$$y = \frac{t^2}{4} - \left(\frac{p^2}{4} - q\right),$$

so verwandelt sich die Resolvente (4) in eine Gleichung in t, welche vom 6ten Grade ist, die aber nur gerade Potenzen von t enthält. Die Lösung dieser Gleichung ist nicht schwieriger, als die Lösung von (4), und man kann sie statt der letzteren zur Resolvente nehmen. Dann gehen die Gleichungen (5), in welche die vorgelegte Gleichung zerfällt, über in

$$x^2 + \left(\frac{p+t}{2}\right)x + \tfrac{1}{2}\left(\frac{t^2}{4} - \frac{p^2}{4} + q\right) + \frac{\frac{p}{2}\left(\frac{t^2}{4} - \frac{p^2}{4} + q\right) - r}{2t} = 0,$$

$$x^2 + \left(\frac{p-t}{2}\right)x + \tfrac{1}{2}\left(\frac{t^2}{4} - \frac{p^2}{4} + q\right) - \frac{\frac{p}{2}\left(\frac{t^2}{4} - \frac{p^2}{4} + q\right) - r}{2t} = 0,$$

und daraus erhält man die vier Wurzeln der vorgelegten Gleichung, sobald man eine einzige Wurzel der Resolvente in t kennt.

Die erstere der beiden letzten Gleichungen hat die Wurzeln x_0 und x_2, die zweite die Wurzeln x_1 und x_3; es ist daher

$$x_0 + x_2 = -\frac{p+t}{2}, \; x_1 + x_3 = -\frac{p-t}{2},$$

und durch Subtraction dieser Formeln ergiebt sich

$$-t = x_0 - x_1 + x_2 - x_3.$$

Danach ist die Wurzel der Resolvente in t eine lineare Function der Wurzeln der vorgelegten Gleichung, und diese Function nimmt in der That in Folge der Substitutionen der Wurzeln sechs Werthe an, von denen je zwei einander entgegengesetzt gleich sind.

503. Methode von Lagrange. — Nach der in No. 489 und 490 dargelegten allgemeinen Theorie kann man die vier Wurzeln der Gleichung vierten Grades rational durch eine Function dieser Wurzeln ausdrücken, die so beschaffen ist, dass die 1.2.3.4 Werthe, welche man daraus durch die Substitutionen der Wurzeln herleitet, von einander verschieden sind. Eine Function dieser Art hängt von einer Gleichung vom Grade 24 ab. Die Betrachtung der Methode von Ferrari hat uns aber gezeigt, dass zur Auflösung der Gleichung vierten Grades schon die Kenntniss einer Function der Wurzeln genügt, welche nur drei verschiedene Werthe, oder welche sechs Werthe hat, von denen je zwei einander entgegengesetzt gleich sind.

Die Gleichung, von welcher eine solche Function der Wurzeln der vorgelegten Gleichung abhängt, direkt zu bilden und sodann diese Wurzeln zu bestimmen, ermöglicht eine neue von Lagrange herrührende Methode, die wir jetzt entwickeln wollen.

Wir bezeichnen die vier Wurzeln der vorgelegten Gleichung

$$(1). \qquad x^4 + px^3 + qx^2 + rx + s = 0$$

mit x_0, x_1, x_2, x_3. Die einfachste Function dieser Wurzeln, welche nur drei Werthe annehmen kann, ist $x_0x_2 + x_1x_3$. Wir setzen daher

$$y = x_0x_2 + x_1x_3$$

und suchen zunächst den Werth von y zu ermitteln, oder vielmehr die Gleichung dritten Grades zu bilden, von welcher y abhängt.

Sind y_0, y_1, y_2 die drei Werthe, welche y annehmen kann, so hat man

$$y_0 = x_0 x_2 + x_1 x_3\,,\ y_1 = x_0 x_3 + x_1 x_2\,,\ y_2 = x_0 x_1 + x_2 x_3\,,$$

und die Gleichung in y ist

$$(2).\quad y^3 - (y_0 + y_1 + y_2) y^2 + (y_0 y_1 + y_0 y_2 + y_1 y_2) y - y_0 y_1 y_2 = 0.$$

Die Coefficienten dieser Gleichung (2) sind symmetrische Functionen der Wurzeln der Gleichung (1) und können folglich rational durch die Coefficienten p, q, r, s ausgedrückt werden. Man hat

$$y_0 + y_1 + y_2 = (x_0 x_1 + x_0 x_2 + x_0 x_3 + x_1 x_2 + x_1 x_3 + x_2 x_3) = q,$$

$$y_0 y_1 + y_0 y_2 + y_1 y_2$$

$$= (x_0 + x_1 + x_2 + x_3)(x_0 x_1 x_2 + x_0 x_1 x_3 + x_0 x_2 x_3 + x_1 x_2 x_3)$$

$$- 4 x_0 x_1 x_2 x_3 = pr - 4s,$$

$$y_0 y_1 y_2 = x_0 x_1 x_2 x_3$$

$$\times [(x_0 + x_1 + x_2 + x_3)^2 - 4(x_0 x_1 + x_0 x_2 + x_0 x_3 + x_1 x_2 + x_1 x_3 + x_2 x_3)]$$

$$+ (x_0 x_1 x_2 + x_0 x_1 x_3 + x_0 x_2 x_3 + x_1 x_2 x_3)^2 = s(p^2 - 4q) + r^2;$$

die Resolvente in y ist somit

$$(3).\quad y^3 - q y^2 + (pr - 4s) y - [s(p^2 - 4q) + r^2] = 0.$$

Da diese Gleichung vom dritten Grade ist, so können wir sie auflösen. Sehen wir jetzt, wie man weiter die Werthe der Wurzeln x_0, x_1, x_2, x_3 erhält.

Ist y_0 irgend eine Wurzel der Gleichung (3), so hat man

$$x_0 x_2 + x_1 x_3 = y_0\,;$$

ausserdem ist

$$x_0 x_2 \times x_1 x_3 = s\,;$$

folglich sind $x_0 x_2$ und $x_1 x_3$ die Wurzeln der Gleichung zweiten Grades

$$(4).\quad z^2 - y_0 z + s = 0.$$

Diese Gleichung habe die Wurzeln z_0 und z_1; dann ist

$$x_0 x_2 = z_0\,,\ x_1 x_3 = z_1\,,$$

und aus den so erhaltenen Werthen der Functionen $x_0 x_2$ und $x_1 x_3$ lassen sich die Summen $x_0 + x_2$ und $x_1 + x_3$ rational zusammensetzen. Man hat nämlich

$$x_1 x_3 (x_0 + x_2) + x_0 x_2 (x_1 + x_3) = -r\,,$$

oder

$$z_1 (x_0 + x_2) + z_0 (x_1 + x_3) = -r\,;$$

ferner ist

$$(x_0 + x_2) + (x_1 + x_3) = -p,$$

mithin

$$x_0 + x_2 = \frac{r - p z_1}{z_1 - z_0}, \quad x_1 + x_3 = \frac{p z_0 - r}{z_1 - z_0}.$$

Da man jetzt $x_0 + x_2$ und $x_0 x_2$, sowie $x_1 + x_3$ und $x_1 x_3$ kennt, so kann man zwei Gleichungen zweiten Grades bilden, von denen die erste die Wurzeln x_0 und x_2, die zweite die Wurzeln x_1 und x_3 hat. Die vorgelegte Aufgabe kann somit als gelöst angesehen werden.

504. Die Auflösung der Gleichung vierten Grades lässt sich leichter mittels einer Resolvente ausführen, deren Wurzel linear aus den Wurzeln der vorgelegten Gleichung zusammengesetzt ist und sechs Werthe hat, von denen je zwei einander entgegengesetzt gleich sind.

Es sei

$$t = x_0 - x_1 + x_2 - x_3.$$

Da diese Function sechs Werthe hat, so hängt sie von einer Gleichung 6ten Grades ab. Nun sind aber je zwei Werthe von t einander entgegengesetzt gleich; folglich wird der Grad der Gleichung in t auf 3 reducirt, wenn man

$$t^2 = \vartheta$$

setzt. Man kann die Gleichung in ϑ direct bilden, da man die Zusammensetzung ihrer Wurzeln kennt. Man kann sie aber auch aus der Resolvente (3) in y herleiten. Es ergiebt sich nämlich leicht, dass man

$$y = \frac{\vartheta - p^2 + 4q}{4}$$

hat; die Resolvente in ϑ ist daher

$$(5). \quad \begin{cases} \vartheta^3 - (3p^2 - 8q)\vartheta^2 + (3p^4 - 16p^2q + 16q^2 + 16pr - 64s)\vartheta \\ \quad - (p^3 - 4pq + 8r)^2 = 0. \end{cases}$$

Die vier Wurzeln x_0, x_1, x_2, x_3 der vorgelegten Gleichung lassen sich nun zwar durch eine einzige Wurzel dieser Gleichung (5) ausdrücken. Man erhält aber weit einfachere Resultate, wenn man die drei Wurzeln von (5) sämmtlich anwendet.

Diese drei Wurzeln seien ϑ_0, ϑ_1, ϑ_2; dann hat man

$$(6).\quad \begin{cases} x_0 - x_1 + x_2 - x_3 = \sqrt{\vartheta_0}, \\ x_0 - x_1 - x_2 + x_3 = \sqrt{\vartheta_1}, \\ x_0 + x_1 - x_2 - x_3 = \sqrt{\vartheta_2}; \end{cases}$$

ausserdem ist

$$(7)\qquad x_0 + x_1 + x_2 + x_3 = -p,$$

und die Gleichungen (6) und (7) liefern folgende Werthe der vier Wurzeln:

$$(8).\quad \begin{cases} x_0 = \dfrac{-p + \sqrt{\vartheta_0} + \sqrt{\vartheta_1} + \sqrt{\vartheta_2}}{4}, \\ x_1 = \dfrac{-p - \sqrt{\vartheta_0} - \sqrt{\vartheta_1} + \sqrt{\vartheta_2}}{4}, \\ x_2 = \dfrac{-p + \sqrt{\vartheta_0} - \sqrt{\vartheta_1} - \sqrt{\vartheta_2}}{4}, \\ x_3 = \dfrac{-p - \sqrt{\vartheta_0} + \sqrt{\vartheta_1} - \sqrt{\vartheta_2}}{4}. \end{cases}$$

Diese vier Wurzeln können durch die eine Formel

$$(9).\qquad x = \frac{-p + \sqrt{\vartheta_0} + \sqrt{\vartheta_1} + \sqrt{\vartheta_2}}{4}$$

dargestellt werden, da jede Wurzelgrösse zwei entgegengesetzt gleiche Werthe hat. Es tritt hier aber noch eine Schwierigkeit ein. Der Ausdruck von x, welchen die Formel (9) giebt, hat nämlich acht Werthe, während die vorgelegte Gleichung nur vier Wurzeln haben kann. Diese Zweideutigkeit lässt sich indess leicht beseitigen. Man kann einen der beiden Werthe von $\sqrt{\vartheta_0}$ und von $\sqrt{\vartheta_1}$ nach Belieben wählen; sobald aber diese Werthe einmal fixirt sind, ist der Werth der Grösse $\sqrt{\vartheta_2}$ nicht mehr zweideutig. Durch Multiplication der drei Gleichungen (6) erhält man nämlich

$$\begin{aligned} \sqrt{\vartheta_0}\sqrt{\vartheta_1}\sqrt{\vartheta_2} = {} & (x_0^3 + x_1^3 + x_2^3 + x_3^3) \\ & + 2(x_0 x_1 x_2 + x_0 x_1 x_3 + x_0 x_2 x_3 + x_1 x_2 x_3) \\ & - x_0(x_1^2 + x_2^2 + x_3^2) - x_1(x_0^2 + x_2^2 + x_3^2) \\ & - x_2(x_0^2 + x_1^2 + x_3^2) - x_3(x_0^2 + x_1^2 + x_2^2) \\ = {} & 2\Sigma x_0^3 + 2\Sigma x_0 x_1 x_2 - \Sigma x_0 \, \Sigma x_0^2 \\ = {} & -p^3 + 4pq - 8r, \end{aligned}$$

und daraus folgt

$$(10). \qquad \sqrt{\vartheta_2} = \frac{-p^3 + 4pq - 8r}{\sqrt{\vartheta_0}\sqrt{\vartheta_1}}.$$

Die Formel (9) liefert somit genau vier Werthe von x, und diese sind die Wurzeln der vorgelegten Gleichung.

Wir machen noch darauf aufmerksam, dass der Erfolg der Methoden von Ferrari und von Lagrange lediglich darauf beruht, dass man Functionen von vier Veränderlichen bilden kann, welche nur drei Werthe haben.

505. Die Erörterung der besonderen Fälle der Gleichung vierten Grades bietet durchaus keine Schwierigkeit dar. Die Formeln (6) oder (8) liefern ohne Weiteres folgende Resultate:

1⁰. Wenn die Resolvente zwei von Null verschiedene gleiche Wurzeln hat, so hat die vorgelegte Gleichung zwei gleiche Wurzeln; ihre beiden anderen Wurzeln sind von diesen und von einander verschieden.

2⁰. Wenn zwei Wurzeln der Resolvente gleich Null sind, so hat die vorgelegte Gleichung zwei Paare gleicher Wurzeln.

3⁰. Wenn die drei Wurzeln der Resolvente einander gleich, aber von Null verschieden sind, so hat die vorgelegte Gleichung drei gleiche Wurzeln.

4⁰. Wenn die drei Wurzeln der Resolvente sämmtlich gleich Null sind, so sind die vier Wurzeln der vorgelegten Gleichung einander gleich.

Wenn die Coefficienten p, q, r, s reell sind, so lehrt die Natur der Wurzeln der Resolvente diejenige der Wurzeln der vorgelegten Gleichung kennen.

Wenn die drei Wurzeln der Resolvente reell sind, und wenn keine von ihnen negativ ist, so geht aus den Formeln (8) hervor, dass die vorgelegte Gleichung vier reelle Wurzeln hat. Hat die Resolvente aber eine oder zwei negative Wurzeln, so sind die vier Wurzeln der vorgelegten Gleichung complex: Jedoch werden zwei dieser Wurzeln reell und gleich, wenn die Resolvente zwei gleiche negative Wurzeln besitzt. Da der letzte Term der Resolvente (5) niemals positiv ist, so kann dieselbe eine einzige negative Wurzel nur in dem Falle haben, in welchem sie eine Wurzel Null hat. Wenn die Resolvente zwei complexe Wurzeln besitzt, so kann man in den Formeln (8) $\sqrt{\vartheta_0}$ und $\sqrt{\vartheta_1}$ als conjugirte complexe Grössen und $\sqrt{\vartheta_2}$ als reell ansehen; die

vorgelegte Gleichung hat dann offenbar zwei reelle und zwei complexe Wurzeln.

506. Methoden von Descartes, Tschirnaus und Euler. — Die Methode von Descartes besteht darin, die vorgelegte Gleichung

$$\varphi(x) = x^4 + px^3 + qx^2 + rx + s = 0$$

mit der Gleichung

$$(x^2 + fx + g)(x^2 + f'x + g') = 0$$

zu identificiren, deren Wurzeln als bekannt angesehen werden können.

Anstatt die Methode der unbestimmten Coefficienten anzuwenden, wie es Descartes thut, kann man ausdrücken, dass $x^2 + fx + g$ ein Divisor des ersten Gliedes der vorgelegten Gleichung ist. Zu diesem Zwecke hat man $\varphi(x)$ durch $x^2 + fx + g$ zu dividiren, und die Coefficienten des Restes, welcher vom ersten Grade in x ist, gleich Null zu setzen. Man erhält auf diese Weise zwei Gleichungen zwischen den beiden Unbekannten f und g, und durch Elimination von f oder von g ergiebt sich eine Gleichung 6ten Grades, die man (No. 99) leicht auf eine kubische Gleichung reduciren kann. Diese Methode ist im Grunde von den vorhergehenden nicht verschieden; denn die Resolvente, zu der sie führt, unterscheidet sich von derjenigen von Lagrange nur durch den Factor 2, durch welchen (No. 99) ihre Wurzeln dividirt sind.

Die Methode von Tschirnaus, welche die Gleichung

$$x^4 + px^3 + qx^2 + rx + s = 0$$

durch Anwendung der Transformation

$$y = a + bx + x^2$$

und durch passende Verfügung über die unbestimmten Grössen a und b auf die Form

$$y^4 + Py^2 + Q = 0$$

bringt, haben wir bereits zur Genüge in No. 191 kennen gelernt.

Euler's Methode besteht darin, y aus den beiden Gleichungen

$$x = a + by + cy^2 + dy^3,$$
$$y^4 = e$$

zu eliminiren und die Endgleichung in x mit der vorgelegten

Gleichung zu identificiren. Die Wurzeln der letzteren sind dann durch die Formel

$$x = a + b\sqrt[4]{e} + c\left(\sqrt[4]{e}\right)^2 + d\left(\sqrt[4]{e}\right)^3$$

gegeben. Es kommt also Alles darauf an, die Werthe der unbestimmten Grössen a, b, c, d, e zu ermitteln, von denen eine willkürlich angenommen werden kann.

Ueber die algebraische Auflösung der Gleichungen.

507. Alle Methoden, welche man zur algebraischen Auflösung der Gleichungen anzuwenden versucht hat, und dasselbe würde mit den Methoden der Fall sein müssen, die man noch erdenken könnte, laufen darauf hinaus, die Auflösung der vorgelegten Gleichung abhängig zu machen von der Auflösung einer andern Gleichung, welche leichter als jene zu lösen ist, und deren Wurzeln Functionen der Wurzeln der vorgelegten Gleichung sind.

So kann man die Gleichung zweiten Grades dadurch auflösen, dass man die Function $x_1 - x_0$ ihrer beiden Wurzeln bestimmt. Das Quadrat dieser Function ist eine symmetrische Function, und da deren Werth bekannt ist, so erfolgt die Auflösung der Gleichung durch Ausziehung einer Quadratwurzel.

Auf dieselbe Weise haben wir ferner die Gleichung dritten Grades auflösen können. Wir bestimmten den Werth einer linearen Function der Wurzeln x_0, x_1, x_2, nämlich:

$$t = x_0 + \alpha x_1 + \alpha^2 x_2,$$

wo α eine der complexen Wurzeln der Gleichung $x^3 = 1$ bezeichnet. Die dritte Potenz dieser Function kann durch die Substitutionen der Wurzeln x_0, x_1, x_2 nur zwei verschiedene Werthe annehmen und hängt folglich von einer Gleichung zweiten Grades ab.

Endlich haben wir die Gleichung vierten Grades dadurch aufgelöst, dass wir den Werth einer der beiden Functionen

$$y = x_0 x_2 + x_1 x_3,$$
$$t = x_0 - x_1 + x_2 - x_3$$

ihrer Wurzeln x_0, x_1, x_2, x_3 bestimmten.

Die erste dieser beiden Functionen kann nur drei Werthe annehmen und hängt daher von einer Gleichung dritten Grades

ab, die wir aufzulösen wissen. Die zweite Function kann sechs Werthe annehmen; sie ist daher von einer Gleichung sechsten Grades abhängig, die aber nur gerade Potenzen der Unbekannten enthält und deshalb auf eine Gleichung dritten Grades zurückgeführt werden kann. Wir haben gesehen, dass die Resolvente in t leichter als diejenige in y zur Auflösung der vorgelegten Gleichung führt. Auch ist die daraus hervorgehende Auflösung der Gleichung vierten Grades derjenigen der Gleichung dritten Grades völlig analog. Die Function t kann nämlich in folgender Weise geschrieben werden:

$$t = x_0 + \alpha x_1 + \alpha^2 x_2 + \alpha^3 x_3,$$

wenn durch α die reelle Wurzel -1 der Gleichung $x^4 = 1$ dargestellt wird.

Die vorstehenden Resultate bilden den Ausgangspunkt der schon mehrfach erwähnten Untersuchungen von Lagrange, welche in den Mémoires de l'Académie de Berlin (1770 u. 1771) und im Auszuge in Lagrange's Traité de la Résolution des équations numériques, Note XIII (3. Ausgabe p. 242) veröffentlicht sind. Lagrange sucht darin die Auflösung der Gleichung n^{ten} Grades, deren Wurzeln $x_0, x_1, x_2, \ldots, x_{n-1}$ sind, durch Anwendung einer Function von der Form

$$t = x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-2} x_{n-2} + \alpha^{n-1} x_{n-1}$$

auszuführen, in welcher α eine Wurzel der Gleichung $x^n = 1$ bezeichnet.

Obgleich diese Untersuchungen nicht zur Auflösung der allgemeinen Gleichungen, deren Grad grösser als 4 ist, haben führen können — eine Aufgabe, deren Unmöglichkeit jetzt in aller Strenge erwiesen ist —, so sind Lagrange's Entwicklungen doch von grosser Wichtigkeit, und wir wollen sie deshalb hier vorführen. Dabei werden wir den von Lagrange selbst eingeschlagenen Weg verfolgen und zunächst den Fall behandeln, in welchem der Grad der Gleichung eine Primzahl, sodann den Fall, in welchem dieser Grad eine zusammengesetzte Zahl ist.

Gleichungen, deren Grad eine Primzahl ist

508. Wir bezeichnen mit

$$x_0, x_1, x_2, \ldots, x_{n-1}$$

die n Wurzeln einer Gleichung

(1). $$V = 0,$$

deren Grad n eine Primzahl ist, mit α irgend eine Wurzel der Gleichung $x^n = 1$ und setzen

(2). $$t = x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1}.$$

Wenn α nicht gleich 1 ist, so sind die Potenzen von α, nämlich

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1},$$

da n eine Primzahl ist, die n Wurzeln der Gleichung $x^n = 1$ und folglich von einander verschieden. Die Function t wird daher, wie wir schon in No. 482 bemerkt haben, durch die Substitutionen der Wurzeln $1 . 2 . 3 \ldots n$ verschiedene Werthe annehmen, also von einer Gleichung vom Grade

$$1 . 2 \ldots n$$

abhängen, die man nach der Methode der No. 180 bilden kann, da man die Zusammensetzung ihrer Wurzeln kennt. Den Entwicklungen der No. 482 zufolge lässt sich aber die Auflösung dieser Gleichung vom Grade $1 . 2 . 3 \ldots n$ auf die Auflösung einer Gleichung $(n-1)^{\text{ten}}$ Grades zurückführen, deren Coefficienten von einer Gleichung vom Grade $1 . 2 . 3 \ldots (n-2)$ abhängen.

Bezeichnet nämlich z der Reihe nach alle Indices

$$0, 1, 2, \ldots, (n-1),$$

bis auf Vielfache von n, die man vernachlässigt, so ist die Ausführung der cyclischen Substitution

$$\binom{z+1}{z}$$

an der Function t gleichbedeutend (No. 482) mit der Multiplication von t mit α, und daraus geht hervor, dass die Gleichung, von welcher t abhängt, nur solche Potenzen von t enthält, deren Exponenten durch n theilbar sind. Der Grad dieser Gleichung wird daher auf $1 . 2 . 3 \ldots (n-1)$ erniedrigt werden, wenn man

$$\Theta = t^n$$

setzt. Es seien

(3). $$\Theta_0, \Theta_1, \Theta_2, \ldots, \Theta_{n-2}$$

die Resultate, die man erhält, wenn man in dem Ausdrucke

(4). $$\Theta = (x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots \alpha^{n-1} x_{n-1})^n$$

α durch jede der Wurzeln

$$\alpha, \beta, \gamma, \ldots, \omega$$

der Gleichung

$$\frac{x^n - 1}{x - 1} = 0$$

ersetzt.

In No. 482 haben wir gesehen, dass wenn r eine primitive Wurzel der Primzahl n bezeichnet, die Grössen (3) eben die Werthe sind, welche Θ annimmt, wenn man in dieser Function die $n - 2$ Potenzen der cyclischen Substitution

$$\binom{rz}{z}$$

ausführt, und aus dieser Thatsache zogen wir den Schluss, dass jede symmetrische Function D der Grössen (3) durch die beiden cyclischen Substitutionen

$$\binom{z+1}{z}, \quad \binom{rz}{z}$$

keine Aenderung erleidet.

Dies vorausgesetzt, kann jede beliebige Substitution als das Produkt von drei Substitutionen angesehen werden, nämlich als Produkt: 1⁰ einer Potenz von $\binom{z+1}{z}$; 2⁰ einer Potenz von $\binom{rz}{z}$, welche den Index 0 nicht versetzt; 3⁰ einer Substitution, welche keinen der beiden Indices 0 und 1 versetzt. Die beiden ersten dieser Substitutionen werden keine Aenderung in D hervorbringen; man erhält somit alle verschiedenen Werthe dieser Function, wenn man die $1 . 2 . 3 \ldots (n-2)$ Substitutionen der $n-2$ Indices $2, 3, \ldots, (n-1)$ vollzieht. Stellt nun

$$(5) \qquad \Theta^{n-1} + P_1 \Theta^{n-2} + P_2 \Theta^{n-3} + \cdots + P_{n-2}\Theta + P_{n-1} = 0$$

die Gleichung dar, welche die $n - 1$ Werthe (3) von Θ zu Wurzeln hat, so hängt jeder der Coefficienten P_1, P_2, u. s. w. von einer Gleichung vom Grade $1 . 2 . 3 \ldots (n-2)$ ab, und da man die Zusammensetzung ihrer Wurzeln kennt, so kann man diese verschiedenen Gleichungen nach der Methode der No. 180 bilden. Man erkennt aber auf der Stelle, dass alle diese Coefficienten $P_1, P_2, \ldots$ nur von einer Gleichung vom Grade $1.2.3 \ldots (n-2)$ abhängen. Dieselben sind nämlich offenbar ähnliche Functionen der Wurzeln $x_0, x_1, \ldots, x_{n-1}$ der vorge-

legten Gleichung, und wenn der Werth einer dieser Functionen gegeben ist, so lassen sich die Werthe der übrigen daraus rational herleiten.

Sehen wir jetzt, wie man die Gleichung, von welcher P_1 abhängt, bilden und die übrigen Coefficienten P_2, P_3, u. s. w. als Functionen von P_1 ausdrücken kann. Man berechne die Gleichung vom Grade $1 . 2 . 3 \ldots (n-1)$, welche alle Werthe von Θ zu Wurzeln hat, und deren Coefficienten als unveränderliche Functionen der Wurzeln der vorgelegten Gleichung rational durch die Coefficienten derselben ausgedrückt werden können. Das erste Glied dieser vollständigen Gleichung in Θ ist durch das erste Glied der Gleichung (5) theilbar. Diese Division ist auf die gewöhnliche Weise auszuführen, und die $n-1$ Terme des Restes sind gleich Null zu setzen. Die $n-2$ ersten der so erhaltenen Gleichungen dienen dazu, die Coefficienten P_2, P_3, u. s. w. durch P_1 auszudrücken, und wenn man die auf diese Weise gefundenen Werthe von P_2, P_3, u. s. w. in die $(n-1)^{\text{te}}$ Gleichung einsetzt, so gelangt man zur Gleichung vom Grade $1 . 2 . 3 \ldots (n-2)$ in P_1.

Die Anwendung der vorstehenden Theorie macht vom 5ten Grade an fast unausführbare Rechnungen erforderlich. Lagrange suchte dieselben zu vereinfachen und ersann in der That einen geistreichen Kunstgriff, um die Coefficienten der Gleichung (5) durch die Wurzeln x_0, x_1, u. s. w. auszudrücken. Dies Verfahren wollen wir jetzt darlegen.

Um den Ausdruck von Θ zu erhalten, hat man die Grösse

$$x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1}$$

auf die n^{te} Potenz zu erheben. Führt man diese Rechnung aus und drückt die Exponenten von α unter n hinab, so ergiebt sich ein Resultat von der Form

$$(6). \qquad \Theta = \xi_0 + \alpha \xi_1 + \alpha^2 \xi_2 + \cdots + \alpha^{n-1} \xi_{n-1}.$$

Die Formel (6) liefert die Werthe von $\Theta_0, \Theta_1, \ldots, \Theta_{n-2}$, wenn man für α jede der complexen Wurzeln $\alpha, \beta, \gamma, \ldots \omega$ der Gleichung $x^n = 1$ substituirt. Ersetzt man ferner α durch 1, so hat das zweite Glied der Gleichung (6) den Werth

$$(x_0 + x_1 + \cdots + x_{n-1})^n \text{ oder } A^n,$$

wenn A die bekannte Summe der Wurzeln der vorgelegten Gleichung (1) bezeichnet. Es ist daher

$$\begin{aligned}
A^n &= \xi_0 + \xi_1 + \xi_2 + \cdots + \xi_{n-1}, \\
\Theta_0 &= \xi_0 + \alpha\,\xi_1 + \alpha^2\,\xi_2 + \cdots + \alpha^{n-1}\,\xi_{n-1}, \\
\Theta_1 &= \xi_0 + \beta\,\xi_1 + \beta^2\,\xi_2 + \cdots + \beta^{n-1}\,\xi_{n-1}, \\
&\cdots\cdots\cdots\cdots\cdots\cdots, \\
\Theta_{n-2} &= \xi_0 + \omega\,\xi_1 + \omega^2\,\xi_2 + \cdots + \omega^{n-1}\,\xi_{n-1}.
\end{aligned}$$

Addirt man diese Gleichungen und bezeichnet die Summe der Wurzeln der Gleichung (5) mit S_1, so erhält man mit Rücksicht auf die Eigenschaften der Wurzeln α, β, u. s. w.

$$A^n + S_1 = n\,\xi_0\,,$$

oder

$$S_1 = n\,\xi_0 - A^n\,.$$

Allgemein möge S_ν die Summe der ν^{ten} Potenzen der Wurzeln der Gleichung (5) bezeichnen. Wir erheben den Ausdruck (6) auf die ν^{te} Potenz, drücken die Exponenten von α unter n hinab, und stellen das Resultat durch

$$\Theta^\nu = \xi_0^{(\nu)} + \alpha\,\xi_1^{(\nu)} + \alpha^2\,\xi_2^{(\nu)} + \cdots + \alpha^{n-1}\,\xi_{n-1}^{(\nu)}$$

dar. Wird jetzt α der Reihe nach durch $1, \alpha, \beta, \ldots, \omega$ ersetzt und die Summe aller so erhaltenen Resultate gebildet, so folgt

$$A^{\nu n} + S_\nu = n\,\xi_0^{(\nu)}\,,$$

oder

$$S_\nu = n\,\xi_0^{(\nu)} - A^{\nu n}.$$

Auf diese Weise kann man die Summen S_2, S_3, ..., S_{n-1} als Functionen der Wurzeln $x_0, x_1, \ldots, x_{n-1}$ darstellen, und daraus ergeben sich weiter folgende Werthe der Coefficienten P_1, P_2, u. s. w. der Gleichung (5):

$$\begin{aligned}
P_1 &= -\,(n\xi_0 - A^n), \\
P_2 &= +\,\frac{(n\,\xi_0 - A^n)^2}{2} - \frac{(n\,\xi_0^{(2)} - A^{2n})}{2}, \\
P_3 &= -\,\frac{(n\,\xi_0 - A^n)^3}{2\,.\,3} + \frac{(n\,\xi_0 - A^n)\;(n\,\xi_0^{(2)} - A^{2n})}{2} - \frac{(n\,\xi_0^{(3)} - A^{3n})}{3}, \\
&\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

Wir haben jetzt die Coefficienten P_1, P_2 u. s. w. der Gleichung (5) durch die Wurzeln $x_0, x_1, \ldots, x_{n-1}$ der vorgelegten Gleichung ausgedrückt. Vollführt man in dem Ausdrucke eines dieser Coefficienten, z. B. in demjenigen von P_1, alle möglichen

Substitutionen der Wurzeln, so erhält man nur $1 \,.\, 2 \,.\, 3 \ldots (n-2)$ verschiedene Werthe. Man kann auf diese Weise die Gleichung in P_1 direkt bilden und sodann nach dem oben dargelegten Verfahren die übrigen Coefficienten rational durch P_1 ausdrücken.

Wenn man nur ein Werthsystem der Coefficienten P_1, P_2, u. s. w. kennt und die entsprechende Gleichung $(n-1)^{\text{ten}}$ Grades in Θ auflösen kann, so ergiebt sich daraus unmittelbar, wie wir jetzt zeigen wollen, die Auflösung der vorgelegten Gleichung.

Unter der Voraussetzung, die wir hier machen, sind die Grössen $\Theta_0, \Theta_1, \ldots, \Theta_{n-1}$ bekannt, und die Gleichung (4) liefert, wenn $\alpha, \beta, \gamma, \ldots, \omega$ an die Stelle von α gesetzt wird:

$$(7). \quad \begin{cases} x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1} = \sqrt[n]{\Theta_0}, \\ x_0 + \beta x_1 + \beta^2 x_2 + \cdots + \beta^{n-1} x_{n-1} = \sqrt[n]{\Theta_1}, \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot, \\ x_0 + \omega x_1 + \omega^2 x_2 + \cdots + \omega^{n-1} x_{n-1} = \sqrt[n]{\Theta_{n-2}}. \end{cases}$$

Ausserdem hat man

$$x_0 + x_1 + x_2 + \cdots + x_{n-1} = A.$$

Durch Addition dieser Gleichungen ergiebt sich mit Bezugnahme auf die Eigenschaften der Wurzeln α, β, u. s. w.

$$(8). \quad x_1 = \frac{A + \sqrt[n]{\Theta_0} + \sqrt[n]{\Theta_1} + \cdots + \sqrt[n]{\Theta_{n-2}}}{n}.$$

Addirt man dieselben Gleichungen, nachdem man sie beziehungsweise mit $\alpha^\nu, \beta^\nu, \ldots, \omega^\nu$ und 1 multiplicirt hat, so folgt

$$(9). \quad x_{n-\nu} = \frac{A + \alpha^\nu \sqrt[n]{\Theta_0} + \beta^\nu \sqrt[n]{\Theta_1} + \cdots + \omega^\nu \sqrt[n]{\Theta_{n-2}}}{n}.$$

Da aber Nichts den Werth jeder Wurzelgrösse, den man zu nehmen hat, bestimmt, so ist das zweite Glied der Formel (9) vom zweiten Gliede von (8) nicht verschieden. Die n Wurzeln der vorgelegten Gleichung sind daher durch die eine Formel

$$(10). \quad x = \frac{A + \sqrt[n]{\Theta_0} + \sqrt[n]{\Theta_1} + \cdots + \sqrt[n]{\Theta_{n-2}}}{n}$$

gegeben. Zwar liefert diese Formel der Vieldeutigkeit der Wurzelgrössen wegen n^{n-1} Werthe für x; die hieraus hervorgehende Unbestimmtheit lässt sich aber leicht beseitigen. Die ersten Glieder der Gleichungen (7) sind nämlich ähnliche Functionen der

Wurzeln x_0, x_1, u. s. w. Man kann also, wenn eine dieser Functionen gegeben ist, alle übrigen daraus rational herleiten. So kann man $\sqrt[n]{\Theta_1}$, $\sqrt[n]{\Theta_2}$, ..., $\sqrt[n]{\Theta_{n-2}}$ rational durch $\sqrt[n]{\Theta_0}$ ausdrücken, und dann liefert die Formel (10), wie es auch der Fall sein muss, nur n Werthe für x.

Diese Methode führt die Auflösung der Gleichung 5ten Grades auf die einer Gleichung 4ten Grades zurück, deren Coefficienten von einer Gleichung 6ten Grades abhängen.

Gleichungen, deren Grad eine zusammengesetzte Zahl ist.

509. Die vorhergehende Entwicklung lässt sich auf die Gleichungen, deren Grad eine zusammengesetzte Zahl ist, nicht anwenden, und es ist hier erforderlich, neue Betrachtungen anzustellen. Die Methode, welche Lagrange für diesen Fall vorgeschlagen hat, läuft im Grunde darauf hinaus, die vorgelegte Gleichung

$$V = 0, \tag{1}$$

deren Grad m gleich dem Produkte einer Zahl p in eine Primzahl n ist, in n Gleichungen p^{ten} Grades zu zerlegen. Zu diesem Zwecke ist nur die Auflösung einer Gleichung vom Grade

$$\frac{1 \cdot 2 \ldots m}{(n-1)\, n\, (1 \cdot 2 \ldots p)^n}$$

und die einer Gleichung $(n-1)^{\text{ten}}$ Grades erforderlich, während, wenn man die Zerlegung nach der gewöhnlichen Methode ausführen wollte, eine Gleichung vom Grade

$$\frac{m\,(m-1) \ldots (m-p+1)}{1 \cdot 2 \ldots p}$$

aufzulösen sein würde.

Hat man die Gleichung (1) in n Gleichungen p^{ten} Grades zerlegt, so kann man auf jede der letzteren, falls p eine Primzahl ist, die oben dargelegte Methode anwenden. Ist dagegen p gleich dem Produkte einer Zahl p' in eine Primzahl n', $p = n'p'$, so hat man jede Gleichung p^{ten} Grades ebenso wie die vorgelegte Gleichung (1) zu behandeln und dadurch in n' Gleichungen vom Grade p' zu zerlegen, u. s. w. Betrachten wir die Methode jetzt in ihren Einzelheiten.

Es sei $m = np$, wo n eine Primzahl bedeutet. Wir setzen, wie früher,

$$t = x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{m-1} x_{m-1};$$

darin bezeichnen $x_0, x_1, \ldots, x_{m-1}$ die m Wurzeln der Gleichung (1) und α eine Wurzel von $x^m = 1$, die aber auch der Gleichung $x^n = 1$ angehört. Da man dann allgemein

$$\alpha^{n+k} = \alpha^k$$

hat, so lässt sich der vorhergehende Werth von t folgendermassen schreiben:

$$\begin{aligned} t = & [x_0 + x_n + x_{2n} + \cdots + x_{(p-1)n}] \\ & + \alpha [x_1 + x_{n+1} + x_{2n+1} + \cdots + x_{(p-1)n+1}] \\ & + \cdots\cdots\cdots\cdots \\ & + \alpha^{n-1} [x_{n-1} + x_{2n-1} + \cdots + x_{pn-1}], \end{aligned}$$

oder

$$t = X_0 + \alpha X_1 + \alpha^2 X_2 + \cdots + \alpha^{n-1} X_{n-1},$$

wenn der Kürze wegen

$$(2). \quad \begin{cases} X_0 = x_0 + x_n + x_{2n} + \cdots + x_{(p-1)n}, \\ X_1 = x_1 + x_{n+1} + x_{2n+1} + \cdots + x_{(p-1)n+1}, \\ \cdots\cdots\cdots\cdots, \\ X_{n-1} = x_{n-1} + x_{2n-1} + x_{3n-1} + \cdots + x_{pn-1} \end{cases}$$

gemacht wird. Die Gleichung, welche $X_0, X_1, \ldots, X_{n-1}$ zu Wurzeln hat, stellen wir durch

$$(3). \qquad W = 0$$

dar. Auf diese Gleichung (3) können wir die oben für die Gleichungen, deren Grad eine Primzahl ist, dargelegte Methode anwenden. Wir machen $\Theta = t^n$, oder

$$(4). \qquad \Theta = (X_0 + \alpha X_1 + \alpha^2 X_2 + \cdots + \alpha^{n-1} X_{n-1})^n.$$

Θ hängt von einer Gleichung vom Grade $1 . 2 . 3 \ldots (n-1)$ ab, deren Coefficienten sich rational durch diejenigen der Gleichung (3) ausdrücken lassen, und wenn $\Theta_0, \Theta_1, \ldots, \Theta_{n-2}$ die $n-1$ Werthe darstellen, welche Θ annimmt, wenn man α durch die $n-1$ complexen Wurzeln von $x^n = 1$ ersetzt, so kann man die Gleichung $(n-1)^{\text{ten}}$ Grades bilden, welche diese $n-1$ Werthe von Θ zu Wurzeln hat. Diese Gleichung werde durch

$$(5). \quad \Theta^{n-1} + P_1 \Theta^{n-2} + P_2 \Theta^{n-3} + \cdots + P_{n-2}\Theta + P_{n-1} = 0$$

dargestellt, Ihre Coefficienten P_1, P_2, u. s. w. hängen von einer einzigen Gleichung vom Grade $1 . 2 . 3 \ldots (n-2)$ ab, deren Coefficienten, wie früher gezeigt wurde, rational durch diejenigen der Gleichung (3) ausgedrückt werden können.

Es seien y irgend einer der Coefficienten P_1, P_2, u. s. w. und

(6). $$f(y) = 0$$

die Gleichung vom Grade $1 . 2 . 3 \ldots (n-2)$, von welcher y abhängt. Die Coefficienten dieser Gleichung (6) sind rational durch diejenigen der Gleichung (3) ausdrückbar; die letzteren sind aber nicht bekannt; wir kennen nur die Coefficienten der Gleichung (1). Wir wollen daher jetzt zeigen, wie man eine Gleichung in y bilden kann, deren Coefficienten durch die bekannten Grössen ausgedrückt sind.

$f(y)$ ist eine Function von y, welche die Grössen

$$X_0 , X_1 , \ldots , X_{n-1}$$

symmetrisch enthält, und wenn man darin X_0, X_1, u. s. w. durch ihre Werthe (2) ersetzt, so wird $f(y)$ eine ganze, nicht symmetrische Function der Wurzeln $x_0 , x_1 , \ldots , x_{m-1}$ der Gleichung (1). Führen wir in $f(y)$ alle Substitutionen der Wurzeln

$$x_0 , x_1 , \ldots , x_{m-1}$$

aus und bezeichnen die μ verschiedenen Werthe, welche $f(y)$ auf diese Weise annimmt, mit

$$f_0(y) , f_1(y) , \ldots , f_{\mu-1}(y) ,$$

so ist das Produkt aller dieser Werthe eine symmetrische Function der Wurzeln $x_0 , x_1 , \ldots , x_{m-1}$, mithin rational durch die Coefficienten der vorgelegten Gleichung ausdrückbar. Man hat daher zur Bestimmung von y die Gleichung

(7). $$f_0(y) f_1(y) f_2(y) \ldots f_{\mu-1}(y) = 0 ,$$

deren Coefficienten als bekannt angesehen werden können.

Der Grad der Gleichung (7) ist $1 . 2 . 3 \ldots (n-2) \times \mu$, wenn μ die Anzahl der verschiedenen Werthe bezeichnet, welche $f(y)$ in Folge der Substitutionen der Wurzeln $x_0 , x_1 , \ldots , x_{m-1}$ annimmt. Wir wissen, dass diese Zahl μ ein Divisor des Produkts $1 . 2 . 3 \ldots m$ ist, und wenn man

$$\mu = \frac{1 . 2 . 3 \ldots m}{\nu}$$

macht, so ist ν die Anzahl der Substitutionen, welche der Func-

tion $f(y)$ angehören. Nun erleidet $f(y)$ keine Aenderung, wenn man die Wurzeln, welche in einem der Ausdrücke

$$X_0, X_1, \ldots, X_{n-1}$$

enthalten sind, und ebenso, wenn man die Ausdrücke X_0, X_1, u. s. w. selbst gegeneinander vertauscht. Jede Substitution dagegen, welche einige der in X_1, oder in X_2, oder u. s. w. enthaltenen Wurzeln in eine andere dieser Functionen einführt, ändert offenbar die Function $f(y)$. Daraus ergiebt sich leicht, dass

$$\nu = (1 \cdot 2 \cdot 3 \ldots p)^n \cdot (1 \cdot 2 \ldots n),$$

folglich

$$\mu = \frac{1 \cdot 2 \cdot 3 \ldots m}{(1 \cdot 2 \cdot 3 \ldots n)(1 \cdot 2 \cdot 3 \ldots p)^n}$$

ist. Der Grad der Gleichung (7) ist daher

$$1 \cdot 2 \cdot 3 \ldots (n-2) \frac{1 \cdot 2 \cdot 3 \ldots m}{(1 \cdot 2 \cdot 3 \ldots n)(1 \cdot 2 \ldots p)^n},$$

oder

$$\frac{1 \cdot 2 \cdot 3 \ldots m}{(n-1)\, n\, (1 \cdot 2 \cdot 3 \ldots p)^n},$$

was mit dem in No. 427 bewiesenen Satze (Zusatz II) übereinstimmt.

Kennt man eine einzige Wurzel der Gleichung (7), so erhält man ein Werthsystem der Coefficienten

$$P_1, P_2, \ldots, P_{n-1}$$

der Gleichung (5). Diese Coefficienten sind nämlich ähnliche Functionen der Wurzeln der vorgelegten Gleichung, und können folglich rational durch irgend einen von ihnen und die bekannten Grössen ausgedrückt werden.

Wir haben jetzt die Gleichung (5) aufzulösen, die nur vom Grade $n-1$ ist. Ist dies geschehen, so erhält man leicht die Wurzeln der Gleichung (3). Es seien nämlich

$$\Theta_0, \Theta_1, \Theta_2, \ldots, \Theta_{n-2}$$

die $n-1$ Wurzeln der Gleichung (5). Da diese Werthe von Θ genau dieselben sind, wie diejenigen, die sich aus der Gleichung (4) ergeben, wenn darin α durch jede der complexen Wurzeln von $x^n = 1$ ersetzt wird, so hat man

$$X_0 + \alpha X_1 + \alpha^2 X_2 + \cdots + \alpha^{n-1} X_{n-1} = \sqrt[n]{\Theta_0},$$
$$X_0 + \beta X_1 + \beta^2 X_2 + \cdots + \beta^{n-1} X_{n-1} = \sqrt[n]{\Theta_1},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots,$$
$$X_0 + \omega X_1 + \omega^2 X_2 + \cdots + \omega^{n-1} X_{n-1} = \sqrt[n]{\Theta_{n-2}}.$$

Ausserdem ist die Summe der Wurzeln $X_1, X_2, \ldots, X_n$ bekannt, da sie nichts Anderes als die Summe der Wurzeln $x_0, x_1, \ldots, x_{m-1}$ ist. Wird diese Summe also mit A bezeichnet, so hat man

$$X_0 + X_1 + X_2 + \cdots + X_{n-1} = A.$$

Aus den vorhergehenden Gleichungen erhält man folgenden allgemeinen Ausdruck der Wurzeln X_0, X_1, u. s. w.:

$$X = \frac{A + \sqrt[n]{\Theta_0} + \sqrt[n]{\Theta_1} + \cdots + \sqrt[n]{\Theta_{n-2}}}{n}.$$

Es erübrigt jetzt noch, die Wurzeln x_0, x_1, u. s. w. selbst zu ermitteln. Zu diesem Zwecke haben wir die Gleichung zu betrachten, deren Wurzeln diejenigen Wurzeln der vorgelegten Gleichung sind, welche die Summe X_0, oder X_1, oder u. s. w., z. B. X_0 haben. Diese Gleichung sei

$$x^p - X_0 x^{p-1} + Q_2 x^{p-2} + \cdots + Q_{p-1} x + Q_p = 0.$$

Ihr erstes Glied ist ein Divisor des ersten Gliedes V der vorgelegten Gleichung. Man hat diese Division auf die gewöhnliche Art auszuführen, und die p Terme des Restes gleich Null zu setzen. Die $p-1$ ersten der so erhaltenen p Gleichungen drücken Q_2, Q_3, u. s. w. durch X_0 aus, und die letzte ist sodann von selbst erfüllt. Es liegt auf der Hand, dass Q_2, Q_3, u. s. w. rational durch X_0 ausgedrückt werden, da alle diese Functionen ähnlich sind. Man erhält also endlich durch dieses Verfahren die n Gleichungen p^{ten} Grades, in welche die vorgelegte Gleichung zerlegt werden kann.

Dies ist der Punkt, bis zu welchem die Arbeiten von Lagrange die Frage nach der algebraischen Auflösung der Gleichungen geführt haben. Die Resolvente hat uns die Auflösung der Gleichungen dritten und vierten Grades geliefert. Sie ist aber von keinem Nutzen für die allgemeinen Gleichungen, deren Grad grösser als 4 ist; die Auflösung der letzteren ist ja auch jetzt als unmöglich nachgewiesen. Wir werden jedoch später sehen, dass die Betrachtung der Resolvente von Lagrange zur

algebraischen Auflösung einer sehr umfangreichen Classe von Gleichungen beliebiger Grade führt.

Um dieselbe Zeit, zu welcher Lagrange in Berlin die Abhandlung veröffentlichte, deren wichtigste Resultate wir im Vorstehenden dargelegt haben, beschäftigte sich Vandermonde mit derselben Frage und legte der Pariser Akademie der Wissenschaften eine schöne Arbeit vor, in welcher er durch ganz andere Betrachtungen zu denselben Resultaten wie Lagrange gelangt. Wir müssen uns darauf beschränken, auf Vandermonde's in den Mémoires de l'Académie des Sciences de Paris (1771) abgedruckte Arbeit zu verweisen.

Zweites Kapitel.

Ueber die Unmöglichkeit, allgemeine Gleichungen, deren Grad grösser als 4 ist, algebraisch aufzulösen.

Algebraische Functionen.

510. Die im vorigen Kapitel angestellten Betrachtungen führen uns zu dem Glauben, dass es unmöglich sei, die allgemeinen Gleichungen, deren Grad grösser als 4 ist, algebraisch aufzulösen. Abel gelang es, diese Unmöglichkeit in aller Strenge zu beweisen. Seine Methode wurde später von Wantzel in einigen Punkten noch vereinfacht.

Eine Gleichung algebraisch lösen heisst eine algebraische Function der Coefficienten bilden, welche, für die Unbekannte substituirt, der Gleichung identisch genügt. Um also zu erkennen, ob eine Gleichung algebraisch lösbar sei oder nicht, hat man zuerst die allgemeine Form der algebraischen Functionen zu studiren. Aus den Ergebnissen dieser Betrachtung wird die Unmöglichkeit, die angegebenen Gleichungen algebraisch zu lösen, leicht hervorgehen.

Es seien

$$x_1, x_2, x_3, \ldots, x_k$$

k beliebige unabhängige Grössen und v eine Function derselben. Die Function v ist algebraisch, wenn man sie aus x_1, x_2, u. s. w. durch eine endliche Anzahl der folgenden Operationen bilden kann: 1⁰ Addition oder Subtraction; 2⁰ Multiplication; 3⁰ Division; 4⁰ Ausziehung von Wurzeln, deren Exponenten Primzahlen sind. Wir zählen die Erhebung auf ganze Potenzen und die Ausziehung von Wurzeln, deren Exponenten zusammengesetzte Zahlen sind, nicht mit auf, weil diese Operationen in den erwähnten offenbar enthalten sind.

Ganze Functionen.

511. Wenn die Function v durch die beiden ersten der oben angegebenen vier Operationen gebildet werden kann, so heisst sie eine rationale und ganze oder einfach eine ganze Function.

Wir bezeichnen mit

$$f(x_1, x_2, x_3, \ldots)$$

eine Function, welche durch eine Summe einer beschränkten Anzahl von Termen der Form

$$A x_1^{m_1} x_2^{m_2} \ldots$$

ausgedrückt werden kann, wo A eine Constante und m_1, m_2, u. s. w. ganze positive Exponenten bedeuten. Die mit f bezeichnete Operation liefert der vorstehenden Definition nach eine ganze Function, und man kann allgemein alle ganzen Functionen dadurch entstanden denken, dass diese Operation eine beschränkte Anzahl Male wiederholt wird. Sind v_1, v_2, u. s. w. Functionen von x_1, x_2, u. s. w., welche dieselbe Form wie f haben, so ist offenbar auch die Function

$$f(v_1, v_2, \ldots)$$

von derselben Form. Ausserdem ist $f(v_1, v_2, \ldots)$ der Ausdruck der Functionen, die durch zweimalige Ausführung der Operation $f(x_1, x_2, \ldots)$ entstehen. Daraus geht hervor, dass man ein Resultat von derselben Form erhält, wenn man diese Operation beliebig oft wiederholt, und dass jede ganze Function von x_1, x_2, u. s. w. durch eine Summe von Termen der Form

$$A x_1^{m_1} x_2^{m_2} \ldots$$

ausgedrückt werden kann.

Rationale Functionen.

512. Eine Function v der Grössen $x_1, x_2, x_3, \ldots$ heisst rational, wenn sie durch die drei ersten der oben angegebenen vier Operationen gebildet werden kann.

Sind

$$f(x_1, x_2, x_3, \ldots), \quad F(x_1, x_2, x_3, \ldots)$$

zwei ganze Functionen, so ist der Quotient

$$\frac{f(x_1, x_2, x_3, \ldots)}{F(x_1, x_2, x_3, \ldots)}$$

ein besonderer Fall der gebrochenen rationalen Functionen, und man kann jede rationale Function durch mehrmalige Wiederholung der vorhergehenden Operation entstanden denken. Bezeichnen aber v_1, v_2, u. s. w. mehrere Functionen von der Form

$$\frac{f(x_1, x_2, \ldots)}{F(x_1, x_2, \ldots)},$$

so kann die Function

$$\frac{f(v_1, v_2, \ldots)}{F(v_1, v_2, \ldots)}$$

offenbar auf dieselbe Form reducirt werden. Daraus folgt, dass jede rationale Function sich auf die Form

$$\frac{f(x_1, x_2, \ldots)}{F(x_1, x_2, \ldots)}$$

bringen lässt, wo f und F ganze Functionen bezeichnen.

Eintheilung der nicht rationalen algebraischen Functionen.

513. Es sei

$$f(x_1, x_2, \ldots)$$

eine beliebige rationale Function. Offenbar wird man jede algebraische Function dadurch erhalten, dass man die mit f bezeichnete Operation mit der mit $\sqrt[m]{\ }$ bezeichneten, wo m eine Primzahl ist, verbindet. Bezeichnen also p_1, p_2, u. s. w. rationale Functionen von x_1, x_2, u. s. w., ferner n_1, n_2, u. s. w. Primzahlen, und macht man

$$p' = f(x_1, x_2, \ldots, \sqrt[n_1]{\ }, \sqrt[n_2]{p_2}, \ldots),$$

so ist p' die Form der algebraischen Functionen, in welchen die mit $\sqrt[m]{\ }$ bezeichnete Operation sich nur auf rationale Functionen bezieht. Die Functionen von der Form p' werden wir mit *Abel* *algebraische Functionen erster Ordnung* nennen.

Sind p_1', p_2', u. s. w. algebraische Functionen erster Ordnung und n_1', n_2', u. s. w. Primzahlen, so ist

$$p'' = f(x_1, x_2, \ldots, \sqrt[n_1]{p_1}, \sqrt[n_2]{p_2}, \ldots, \sqrt[n_1']{p_1'}, \sqrt[n_2']{p_2'}, \ldots)$$

die allgemeine Form der algebraischen Functionen, in denen die mit $\sqrt[m]{}$ bezeichnete Operation sich nur auf rationale oder auf Functionen erster Ordnung bezieht. Die Functionen von der Form p'' sollen algebraische Functionen zweiter Ordnung genannt werden.

Bezeichnen ferner p_1'', p_2'', u. s. w. algebraische Functionen zweiter Ordnung und n_1'', n_2'', u. s. w. Primzahlen, so ist

$$p''' = f(x_1, x_2, \ldots, \sqrt[n_1]{p_1}, \ldots, \sqrt[n_1']{p_1'}, \ldots, \sqrt[n_1'']{p_1''}, \ldots)$$

die allgemeine Form der algebraischen Functionen, in welchen die mit $\sqrt[m]{}$ bezeichnete Operation sich nur auf rationale und auf Functionen der beiden ersten Ordnungen bezieht. Die Functionen von der Form p''' sollen algebraische Functionen dritter Ordnung heissen.

So fortfahrend gelangt man zu den algebraischen Functionen 4ter, 5ter, ..., μ^{ter} Ordnung, und es liegt auf der Hand, dass der allgemeine Ausdruck der Functionen μ^{ter} Ordnung der allgemeine Ausdruck der algebraischen Functionen ist.

Aus dem Vorhergehenden ergiebt sich, dass eine algebraische Function μ^{ter} Ordnung v von der Form

$$v = f(r_1, r_2, \ldots, \sqrt[n_1]{p_1}, \sqrt[n_2]{p_2}, \ldots)$$

ist; darin bezeichnen f immer eine rationale Function, $p_1, p_2, \ldots$ Functionen $(\mu - 1)^{\text{ter}}$ Ordnung, $n_1, n_2, \ldots$ Primzahlen, und r_1, $r_2, \ldots$ Functionen, deren Ordnung gleich $\mu - 1$ oder kleiner als $\mu - 1$ ist.

Man kann offenbar voraussetzen, dass keine der Wurzelgrössen $\sqrt[n_1]{p_1}, \sqrt[n_2]{p_2}, \ldots$ rational durch die übrigen Wurzelgrössen und die Grössen $r_1, r_2, \ldots$ ausdrückbar sei. Wäre dies nämlich mit der Grösse $\sqrt[n_1]{p_1}$ der Fall, so würde man durch Einsetzung ihres Werthes in den Ausdruck von v einen Werth

$$v = f(r_1, r_2, \ldots, \sqrt[n_2]{p_2}, \ldots)$$

erhalten, welcher von derselben Form wie der vorhergehende, aber einfacher als dieser wäre, da er $\sqrt[n_1]{p_1}$ nicht enthielte. Wenn

in gleicher Weise eine der übrig gebliebenen Wurzelgrössen rational durch die übrigen Wurzelgrössen und die Grössen $r_1, r_2, \ldots$ ausgedrückt werden könnte, so könnte man dieselbe aus dem Ausdrucke von v entfernen, der übrigens die alte Form behalten würde, und wenn man so fortfahren könnte, bis alle Wurzelgrössen $\sqrt[n_1]{p_1}, \sqrt[n_2]{p_2}, \ldots$ eliminirt wären, so würde die Ordnung der Function v auf $\mu - 1$ reducirt sein.

Wenn also die Function v wirklich von der μ^{ten} Ordnung ist, so darf man voraussetzen, dass die Anzahl der Wurzelgrössen $\sqrt[n_1]{p_1}, \sqrt[n_2]{p_2}, \ldots$ bereits möglichst klein gemacht ist, dass es also unmöglich ist, eine dieser Grössen als rationale Function der übrigen und der algebraischen Functionen niedrigerer Ordnung auszudrücken. Bezeichnet dann m die Anzahl dieser aus algebraischen Functionen $(\mu - 1)^{\text{ter}}$ Ordnung zu ziehenden Wurzeln, so sagen wir, die Function v sei von der μ^{ten} Ordnung und vom m^{ten} Grade.

Nach dieser Definition ist eine Function μ^{ter} Ordnung und nullten Grades nichts Anderes, als eine Function $(\mu - 1)^{\text{ter}}$ Ordnung, und eine Function nullter Ordnung eine rationale Function.

Wir sehen somit, dass, wenn v eine algebraische Function μ^{ter} Ordnung und m^{ten} Grades bezeichnet, allgemein

$$v = f(r_1, r_2, \ldots, \sqrt[n]{p})$$

ist, wo f eine rationale Function, p eine algebraische Function $(\mu - 1)^{\text{ter}}$ Ordnung, n eine Primzahl, und $r_1, r_2, \ldots$ Functionen μ^{ter} Ordnung, aber $(m - 1)^{\text{ten}}$ Grades bezeichnen. Ausserdem kann man nach dem Vorhergehenden immer voraussetzen, dass es unmöglich ist, $\sqrt[n]{p}$ rational durch $r_1, r_2, \ldots$ auszudrücken.

Allgemeine Form der algebraischen Functionen.

514. Im vorstehenden Ausdruck von v bezeichnet f eine rationale Function der Grössen $r_1, r_2, \ldots, \sqrt[n]{p}$. Jede rationale Function mehrerer Grössen kann aber als Quotient zweier ganzen Functionen dargestellt werden. Wir können daher

$$v = \frac{\varphi(r_1, r_2, \ldots, \sqrt[n]{p})}{\psi(r_1, r_2, \ldots, \sqrt[n]{p})}$$

setzen, worin φ und ψ ganze Functionen bezeichnen. Ordnet

man φ und ψ nach Potenzen von $\sqrt[n]{p}$ oder $p^{\frac{1}{n}}$, so erhält man für v einen Werth von der Form

$$v = \frac{s_0 + s_1 p^{\frac{1}{n}} + s_2 p^{\frac{2}{n}} + \cdots + s_\nu p^{\frac{\nu}{n}}}{t_0 + t_1 p^{\frac{1}{n}} + t_2 p^{\frac{2}{n}} + \cdots + t_{\nu'} p^{\frac{\nu'}{n}}} = \frac{S}{T},$$

wo $s_0, s_1, \ldots, s_\nu, t_0, t_1, \ldots, t_{\nu'}$ ganze Functionen von $r_1, r_2, \ldots$ sind.

Es sei nun α eine complexe Wurzel der Gleichung

$$\alpha^n = 1.$$

Wir bezeichnen die $n-1$ Werthe, welche entstehen, wenn $p^{\frac{1}{n}}$ in T der Reihe nach durch

$$\alpha p^{\frac{1}{n}}, \; \alpha^2 p^{\frac{1}{n}}, \; \alpha^3 p^{\frac{1}{n}}, \; \ldots, \; \alpha^{n-1} p^{\frac{1}{n}}$$

ersetzt wird, mit

$$T_1, \; T_2, \; \ldots, \; T_{n-1},$$

und multipliciren beide Terme des Werthes von v mit $T_1 T_2 \ldots T_{n-1}$; es ergiebt sich

$$v = \frac{S T_1 T_2 \ldots T_{n-1}}{T T_1 T_2 \ldots T_{n-1}}.$$

Das Produkt $T T_1 T_2 \ldots T_{n-1}$ kann offenbar durch eine ganze Function von $p, r_1, r_2, \ldots$ ausgedrückt werden; es ist daher eine algebraische Function μ^{ter} Ordnung, deren Grad höchstens $m-1$ ist; wir wollen diese Function mit u bezeichnen. Ebenso ist das Produkt $S T_1 T_2 \ldots T_{n-1}$ eine ganze Function von $r_1, r_2, \ldots$ und $\sqrt[n]{p}$; wir stellen den Werth dieser Function durch

$$u_0 + u_1 p^{\frac{1}{n}} + u_2 p^{\frac{2}{n}} + \cdots + u_i p^{\frac{i}{n}}$$

dar und erhalten

$$v = \frac{u_0 + u_1 p^{\frac{1}{n}} + u_2 p^{\frac{2}{n}} + \cdots + u_i p^{\frac{i}{n}}}{u},$$

oder einfach

$$v = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_i p^{\frac{i}{n}},$$

wenn $q_0, q_1, \ldots$ statt $\frac{u_0}{u}, \frac{u_1}{u}, \ldots$ geschrieben wird; $q_0, q_1, \ldots$ bezeichnen hier rationale Functionen von p und $r_1, r_2, \ldots$ Aus

dem vorhergehenden Ausdrucke von v kann man die Potenzen von $p^{\frac{1}{n}}$, deren Exponenten grösser als $n-1$ sind, entfernen. Bezeichnet nämlich j eine Zahl, welche, durch n dividirt, den Quotienten g und den Rest h liefert, so hat man

$$p^{\frac{j}{n}} = p^g \cdot p^{\frac{h}{n}},$$

und mittels dieser Formel kann man v auf die Form

$$(1). \qquad v = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}}$$

bringen; darin sind $q_0, q_1, \ldots, q_{n-1}$ immer noch rationale Functionen von $p, r_1, r_2, \ldots$, folglich algebraische Functionen μ^{ter} Ordnung, deren Grad höchstens $m-1$ ist; ausserdem sind sie so beschaffen, dass es unmöglich ist, $p^{\frac{1}{n}}$ rational durch die Grössen auszudrücken, von denen sie abhängen.

In dem Ausdrucke (1) von v kann

$$q_1 = 1$$

vorausgesetzt werden. Um dies zu beweisen, nehmen wir zunächst an, q_1 sei von Null verschieden und setzen

$$p_1 = p q_1^n,$$

woraus

$$p = \frac{p_1}{q_1^n} \text{ und } p^{\frac{1}{n}} = \frac{p_1^{\frac{1}{n}}}{q_1}$$

folgt. Dann geht der Ausdruck von v über in

$$v = q_0 + p_1^{\frac{1}{n}} + \frac{q_2}{q_1^2} p_1^{\frac{2}{n}} + \cdots + \frac{q_{n-1}}{q_1^{n-1}} p_1^{\frac{n-1}{n}},$$

oder einfacher in

$$(2). \qquad v = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}},$$

wenn p statt p_1 und $q_2, q_3, \ldots$ statt $\frac{q_2}{q_1^2}, \frac{q_3}{q_1^3}, \ldots$ geschrieben wird.

In diesem neuen Ausdrucke (2) von v, welcher aus (1) dadurch hervorgeht, dass man $q_1 = 1$ macht, bezeichnen die Grössen $q_0, q_2, \ldots$ immer noch algebraische Functionen μ^{ter} Ordnung und $(m-1)^{\text{ten}}$ Grades.

Wir nehmen jetzt an, in dem Ausdrucke (1) von v sei $q_1 = 0$, bezeichnen mit q_k eine der Grössen $q_1, q_2, \ldots$, die von Null verschieden ist, und setzen

$$p_1 = q_k^n p^k;$$

daraus ergiebt sich

$$p_1^{\frac{\alpha}{n}} = q_k^\alpha p^{\frac{k\alpha}{n}}.$$

Da n eine Primzahl und k kleiner als n ist, so lassen sich immer zwei ganze Zahlen α und β von der Beschaffenheit ermitteln, dass

$$k\alpha - n\beta = \lambda$$

ist, worin λ eine beliebig gegebene Zahl bezeichnet. Dann hat man

$$p_1^{\frac{\alpha}{n}} = q_k^\alpha p^\beta p^{\frac{\lambda}{n}},$$

mithin

$$p^{\frac{\lambda}{n}} = q_k^{-\alpha} p^{-\beta} p_1^{\frac{\alpha}{n}}.$$

Im Besonderen und der Voraussetzung nach ist

$$p^{\frac{k}{n}} = \frac{p_1^{\frac{1}{n}}}{q_k}.$$

Die beiden letzten Formeln gestatten es, in den Werth (1) von v statt der Potenzen von $p^{\frac{1}{n}}$ diejenigen von $p_1^{\frac{1}{n}}$ einzusetzen. Durch diese Substitution wird offenbar die Form von p nicht verändert; dagegen erhält $p_1^{\frac{1}{n}}$ die Einheit als Coefficienten; denn in dem ursprünglichen Ausdrucke von v hat $p^{\frac{k}{n}}$ den Coefficienten q_k. Die Ergebnisse unserer bisherigen Betrachtung lassen sich in folgenden Satz zusammenfassen:

Lehrsatz. — Jede algebraische Function μ^{ter} Ordnung und m^{ten} Grades kann auf die Form

$$v = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}}$$

gebracht werden; darin sind n eine Primzahl, q_0, q_2, u. s. w. algebraische Functionen μ^{ter} Ordnung, aber

$(m-1)^{\text{ten}}$ Grades, endlich p eine Function $(\mu-1)^{\text{ter}}$ Ordnung, deren n^{te} Wurzel nicht rational durch die Grössen q_0, q_2, u. s. w. ausgedrückt werden kann.

Eigenschaften der algebraischen Functionen, welche einer gegebenen Gleichung genügen.

515. Wir müssen uns hier die in Nr. 100 gegebenen Definitionen in's Gedächtniss zurückrufen.

Betrachtet man ein ganzes und rationales Polynom

$$x^m + a_1 x^{m-1} + a_2 x^{m-2} + \cdots,$$

dessen Coefficienten a_1, a_2, ... gegebene commensurabele Zahlen sind, so heisst jeder Divisor des Polynoms, dessen Coefficienten commensurabel sind, ein commensurabeler Divisor.

Wenn allgemeiner die Coefficienten a_1, a_2, ... des Polynoms rationale Functionen irgendwelcher als bekannt angesehenen Grössen sind, so heisst jeder Divisor der Polynoms, welcher rationale Functionen der bekannten Grössen zu Coefficienten hat, ein commensurabeler Divisor.

In allen Fällen nennt man eine Gleichung irreductibel, wenn ihr erstes Glied keinen commensurabelen Divisor zulässt.

In der allgemeinen Gleichung beliebigen Grades, deren Coefficienten unbestimmt sind, sind die Coefficienten selbst die bekannten Grössen; diese Gleichung ist nothwendig irreductibel.

Dies vorausgesetzt, sei

$$(1). \quad x^m + a_1 x^{m-1} + a_2 x^{m-2} + \cdots + a_{m-1} x + a_m = 0$$

eine Gleichung m^{ten} Grades, deren Coefficienten als rationale Functionen der bekannten Grössen angesehen werden, und es werde angenommen, die Gleichung sei algebraisch auflösbar.

Nach der oben gegebenen Eintheilung der algebraischen Functionen kann man, wenn die Wurzel x eine algebraische Function μ^{ter} Ordnung der bekannten Grössen ist,

$$(2). \quad x = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}}$$

setzen; darin bezeichnet n eine Primzahl und p eine Function $(\mu-1)^{\text{ter}}$ Ordnung; die Grössen q_0, q_2, ..., q_{n-1} können von der μ^{ten} Ordnung, aber ihr Grad muss kleiner als derjenige von

x sein. Endlich dürfen wir voraussetzen, es sei unmöglich, $p^{\frac{1}{n}}$ rational durch $p, q_0, q_2, \ldots$ auszudrücken.

Wird dieser Ausdruck (2) von x in der Gleichung (1) eingesetzt, so erhält man ein Resultat, welches offenbar auf die Form

$$(3). \qquad r_0 + r_1 p^{\frac{1}{n}} + r_2 p^{\frac{2}{n}} + \cdots + r_{n-1} p^{\frac{n-1}{n}} = 0$$

reducirt werden kann; darin bezeichnen $r_0, r_1, r_2, \ldots, r_{n-1}$ rationale Functionen der Grössen $p, q_0, q_2, \ldots, q_{n-1}$. Wir behaupten nun, die Gleichung (3) erfordere, dass man zu gleicher Zeit

$$r_0 = 0 \;,\; r_1 = 0 \;,\; r_2 = 0 \,, \ldots , r_{n-1} = 0$$

habe. Im entgegengesetzten Falle würden nämlich die beiden Gleichungen

$$z^n - p = 0,$$

$$r_0 + r_1 z + r_2 z^2 + \cdots + r_{n-1} z^{n-1} = 0$$

eine oder mehrere Wurzeln gemeinschaftlich haben. Wäre k die Anzahl dieser Wurzeln, so könnte man eine Gleichung k^{ten} Grades bilden, deren Wurzeln diese k gemeinschaftlichen Wurzeln, und deren Coefficienten rationale Functionen von $p, q_0, q_2, \ldots, q_{n-1}$ wären. Diese Gleichung sei

$$s_0 + s_1 z + s_2 z^2 + \cdots + s_k z^k = 0,$$

und es bezeichne

$$t_0 + t_1 z + t_2 z^2 + \cdots + t_i z^i$$

einen irreductibelen Divisor ihres ersten Gliedes, dessen Coefficienten $t_0, t_1, \ldots, t_i$ rationale Functionen von $p, q_0, q_2, \ldots, q_{n-1}$ seien. Die Gleichung

$$(4). \qquad t_0 + t_1 z + t_2 z^2 + \cdots + t_i z^i = 0$$

hat alle ihre Wurzeln mit

$$(5). \qquad z^n - p = 0$$

gemeinschaftlich; ausserdem ist der Grad i der Gleichung (4) wenigstens gleich 2, da man sonst z oder $p^{\frac{1}{n}}$ rational durch $p, q_0, q_2, \ldots, q_{n-1}$ ausdrücken könnte. Bezeichnet daher z irgendeine Wurzel von (4), α eine Wurzel der Gleichung

$$\alpha^n = 1,$$

so hat die Gleichung (4) wenigstens noch eine Wurzel von der Form αz. Die Gleichung (4) hat also eine Wurzel mit

(6) $$t_0 + t_1 \alpha z + t_2 \alpha^2 z^2 + \cdots + t_i \alpha^i z^i = 0,$$

und folglich auch mit der Gleichung

(7). $$(1 - \alpha^i)\, t_0 + (\alpha - \alpha^i)\, t_1 z + \cdots + (\alpha^{i-1} - \alpha^i)\, t_{i-1} z^{i-1} = 0$$

gemeinschaftlich, welche letztere dadurch entsteht, dass man die mit α^i multiplicirte Gleichung (4) von (6) subtrahirt. Die Gleichung (4) wird aber als irreductibel vorausgesetzt; sie kann mithin keine Wurzel mit der Gleichung (7), die von einem niedrigeren Grade als (4) ist, gemeinschaftlich haben. Daraus geht hervor, dass man nothwendig

$$r_0 = 0\ ,\ r_1 = 0\ ,\ \ldots\ ,\ r_{n-1} = 0$$

hat.

Der letzten Gleichungen wegen wird der Ausdruck (2) von x der vorgelegten Gleichung (1) noch genügen, wenn darin für $p^{\frac{1}{n}}$ jeder der n Werthe

$$p^{\frac{1}{n}}\ ,\ \alpha p^{\frac{1}{n}}\ ,\ \beta p^{\frac{1}{n}}\ ,\ \ldots\ ,\ \omega p^{\frac{1}{n}}$$

substituirt worden ist; $1\ ,\ \alpha\ ,\ \beta\ ,\ \ldots\ ,\ \omega$ bezeichnen die n^{ten} Wurzeln der Einheit. Man erhält auf diese Weise n Wurzeln der Gleichung (1), die wir durch

$$x_1\ ,\ x_2\ ,\ \ldots\ ,\ x_n$$

darstellen, und deren Werthe folgende sind:

(8). $$\begin{cases} x_1 = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}}, \\ x_2 = q_0 + \alpha p^{\frac{1}{n}} + \alpha^2 q_2 p^{\frac{2}{n}} + \cdots + \alpha^{n-1} q_{n-1} p^{\frac{n-1}{n}}, \\ x_3 = q_0 + \beta p^{\frac{1}{n}} + \beta^2 q_2 p^{\frac{2}{n}} + \cdots + \beta^{n-1} q_{n-1} p^{\frac{n-1}{n}}, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ , \\ x_n = q_0 + \omega p^{\frac{1}{n}} + \omega^2 q_2 p^{\frac{2}{n}} + \cdots + \omega^{n-1} q_{n-1} p^{\frac{n-1}{n}}. \end{cases}$$

Diese Wurzeln sind von einander verschieden; denn wenn zwei derselben einander gleich wären, so würde sich eine Gleichung ergeben, welche dieselbe Form wie (3) hätte, und dies führt, wie wir gesehen haben, zu einem Widerspruch. Diese Bemerkung ist übrigens für die folgende Betrachtung von keiner Bedeutung.

Wir addiren jetzt die Gleichungen (8), nachdem wir sie beziehungsweise mit

$$1\,,\,1\,,\,1\,,\,\ldots\,,\,1\,,$$

dann mit

$$1\,,\,\alpha^{n-1}\,,\,\beta^{n-1}\,,\,\ldots\,,\,\omega^{n-1}\,,$$

darauf mit

$$1\,,\,\alpha^{n-2}\,,\,\beta^{n-2}\,,\,\ldots\,,\,\omega^{n-2}\,,$$

u. s. w. multiplicirt haben, und erhalten

$$q_0 = \frac{1}{n}(x_1 + x_2 + x_3 + \cdots\cdots + x_n),$$

$$p^{\frac{1}{n}} = \frac{1}{n}(x_1 + \alpha^{n-1} x_2 + \cdots + \omega^{n-1} x_n),$$

$$q_2 p^{\frac{2}{n}} = \frac{1}{n}(x_1 + \alpha^{n-2} x_2 + \cdots + \omega^{n-2} x_n),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$q_{n-1} p^{\frac{n-1}{n}} = \frac{1}{n}(x_1 + \alpha x_2 + \cdots + \omega x_n).$$

Daraus geht hervor, dass, wenn man die Wurzeln der Einheit als bekannt ansieht, die Grössen

$$p^{\frac{1}{n}}\,,\,q_0\,,\,q_2\,,\,\ldots\,,\,q_{n-1}$$

rationale Functionen der Wurzeln der Gleichung (1) sind. In der That ist allgemein

$$q_\varrho = n^{\varrho-1}\,\frac{x_1 + \alpha^{n-\varrho} x_2 + \beta^{n-\varrho} x_3 + \cdots + \omega^{n-\varrho} x_n}{(x_1 + \alpha^{n-1} x_2 + \beta^{n-1} x_3 + \cdots + \omega^{n-1} x_n)^\varrho}.$$

Es bezeichne nun y irgend eine der Grössen $p^{\frac{1}{n}}, q_0, q_2, \ldots, q_{n-1}$, und es sei

$$(9).\qquad y = s_0 + v^{\frac{1}{r}} + s_2 v^{\frac{2}{r}} + \cdots + s_{r-1} v^{\frac{r-1}{r}},$$

wo $s_0, s_2, \ldots$ Functionen sind, die zwar von derselben Ordnung wie y sein können, deren Grad aber kleiner als derjenige von y ist. Nach dem Vorhergehenden hat man

$$y = \varphi(x_1, x_2, \ldots, x_m),$$

wo φ eine rationale Function bezeichnet, und $x_1, x_2, \ldots, x_m$ die m Wurzeln der Gleichung (1) sind, welche nicht sämmtlich in die Function φ einzugehen brauchen. Ist m' die Anzahl der Werthe, welche diese Function φ in Folge der Substitutionen der

Wurzeln x_1, x_2, ... annimmt, so kann man eine Gleichung m'^{ten} Grades bilden, deren Coefficienten rational aus denjenigen der Gleichung (1) zusammengesetzt, und deren Wurzeln

$$y_1, y_2, \dots y_{m'}$$

die m' Werthe der Function φ sind. Da der Werth (9) von y dieser Gleichung genügen muss, so schliesst man wie früher, dass die Grössen

$$v, s_0, s_2, \dots, s_{r-1}$$

rationale Functionen von y_1, y_2, ..., $y_{m'}$ und folglich auch rationale Functionen von x_1, x_2, ..., x_m sind.

Da sich dieses Schlussverfahren unbegrenzt fortsetzen lässt, so erhalten wir das Resultat:

Wenn eine Gleichung algebraisch lösbar ist, so kann man der Wurzel eine solche Form geben, dass alle algebraischen Functionen, aus denen sie zusammengesetzt ist, rationale Functionen der Wurzeln der vorgelegten Gleichung sind.

Beweis der Unmöglichkeit, die allgemeinen Gleichungen, deren Grad grösser als 4 ist, algebraisch zu lösen.

516. Die Wurzeln einer algebraisch auflösbaren Gleichung haben die eben nachgewiesenen Eigenschaften in allen Fällen, sei es, dass es sich um eine Gleichung handelt, deren Coefficienten bestimmte Werthe haben, oder dass man diese Coefficienten als unbestimmt, die Wurzeln der Gleichung also als irgendwelche in durchaus keinem Zusammenhange stehende Grössen ansieht.

Wir halten uns an die letztere Annahme und wollen jetzt darthun, dass es unmöglich ist, die allgemeinen Gleichungen, deren Grad den 4ten übersteigt, algebraisch aufzulösen.

Dieser Satz ist zuerst in aller Strenge von Abel (Crelle Journ. Bd. 1) bewiesen. Ich lasse den einfacheren Beweis hier folgen, den Wantzel gegeben hat*).

Es sei

*) Ich habe geglaubt, Wantzel's Schlussverfahren wörtlich mittheilen zu müssen; indess habe ich einige Einzelheiten unterdrückt, welche durch die in der Theorie der Substitutionen gegebenen Entwicklungen überflüssig gemacht werden.

$$f(x) = 0$$

eine Gleichung m^{ten} Grades mit unbestimmten Coefficienten. Die m Wurzeln dieser Gleichung bezeichnen wir mit

$$x_1, x_2, \ldots, x_m$$

und nehmen an, dieselben seien rational durch die Coefficienten ausdrückbar.

Wenn die Gleichung $f(x) = 0$ durch den Werth x_1 von x befriedigt wird, ihre Coefficienten mögen sein, welche sie wollen, so muss man, da dann die Wurzeln der Gleichung völlig willkürlich sind, identisch wieder x_1 hervorbringen, wenn man in seinen Ausdruck die jeder Wurzelgrösse entsprechende rationale Function substituirt. Auch muss jede zwischen den Wurzeln bestehende Relation eine Identität sein und gültig bleiben, wenn man diese Wurzeln auf irgend eine Weise gegen einander vertauscht.

Wir bezeichnen die nach der Anordnung der Rechnung erste Wurzel, welche in den Werth von x_1 eingeht, mit y und nehmen an, es sei

$$y^n = p.$$

Dann hängt p unmittelbar von den Coefficienten von $f(x) = 0$ ab und lässt sich durch eine symmetrische Function $F(x_1, x_2, x_3, \ldots)$ der Wurzeln ausdrücken; y ist eine rationale Function $\varphi(x_1, x_2, x_3, \ldots)$ derselben Wurzeln.

Da die Function φ nicht symmetrisch ist — sonst würde sich die n^{te} Wurzel von p genau ausziehen lassen —, so muss sie eine Aenderung erleiden, wenn man zwei Wurzeln, z. B. x_1, x_2, transponirt; die Relation

$$\varphi^n = F$$

wird aber immer erfüllt sein. Da überdies F durch diese Transposition nicht verändert wird, so sind die Werthe von φ Wurzeln der Gleichung $y^n = F$, und man hat

$$\varphi(x_2, x_1, x_3, \ldots) = \alpha\varphi(x_1, x_2, x_3, \ldots),$$

wo α eine n^{te} Wurzel der Einheit bezeichnet.

Durch Transposition der Wurzeln x_1 und x_2 ergiebt sich

$$\varphi(x_1, x_2, x_3, \ldots) = \alpha\varphi(x_2, x_1, x_3, \ldots),$$

und wenn man die beiden letzten Gleichungen in einander multiplicirt, so folgt

$$\alpha^2 = 1.$$

Dieses Resultat beweist, dass die Zahl n, die als Primzahl vorausgesetzt wurde, gleich 2 sein muss. Die erste in den Werth der Unbekannten eingehende Wurzelgrösse ist somit eine Quadratwurzel. In der That zeigt sich dies bei den Gleichungen, die man aufzulösen im Stande ist.

Da die Function φ nur zwei Werthe hat, so erleidet sie durch jede beliebige Transposition eine Aenderung, wird aber (No. 481) durch eine cyclische Substitution von 3 oder von 5 Buchstaben nicht verändert; denn jede dieser Substitutionen ist gleichbedeutend mit einer geraden Anzahl von Transpositionen.

Fahren wir jetzt in der Reihe der Operationen fort, die zur Bildung des Werthes x_1 von x erforderlich sind.

Die erste Wurzelgrösse ist mit den Coefficienten von $f(x) = 0$, d. h. die Function φ ist mit symmetrischen Functionen der Wurzeln zu verbinden. Es geschieht dies mittels der ersten Operationen der Algebra, und man erhält auf diese Weise eine Function der Wurzeln, welche zwei Werthe anzunehmen vermag, welche folglich durch die cyclischen Substitutionen von drei Buchstaben unverändert bleibt. Die folgenden Wurzelgrössen können, wenn sie vom zweiten Grade sind, noch Functionen derselben Art liefern. Gesetzt, man sei zu einer solchen Wurzelgrösse gelangt, dass die äquivalente rationale Function durch diese Substitutionen nicht unverändert bleibt. Wir bezeichnen dieselbe wieder mit

$$y = \varphi(x_1, x_2, x_3, \ldots),$$

und machen in der Gleichung

$$y^n = p$$

$$p = F(x_1, x_2, x_3, \ldots).$$

Diese Function ist nicht symmetrisch; sie erleidet nur durch die cyclischen Substitutionen von drei Buchstaben keine Veränderung. Ersetzt man in φ

$$x_1, x_2, x_3$$

durch

$$x_2, x_3, x_1,$$

so bleibt die Relation

$$\varphi^n = F$$

bestehen, und da F bei dieser Substitution unverändert bleibt, so folgt

$$\varphi(x_2, x_3, x_1, x_4, \ldots) = \alpha\varphi(x_1, x_2, x_3, x_4, \ldots),$$

wo α eine n^{te} Wurzel der Einheit bezeichnet.

Vollzieht man in dieser Gleichung zweimal nach einander die cyclische Substitution

$$(x_1, x_2, x_3),$$

so ergiebt sich

$$\varphi(x_3, x_1, x_2, x_4, \ldots) = \alpha\varphi(x_2, x_3, x_1, x_4, \ldots),$$
$$\varphi(x_1, x_2, x_3, x_4, \ldots) = \alpha\varphi(x_3, x_1, x_2, x_4, \ldots),$$

und durch Multiplication der drei letzten Gleichungen erhält man

$$\alpha^3 = 1.$$

n ist also gleich 3.

Wenn die Anzahl der Grössen x_1, x_2, x_3, x_4, u. s. w. grösser als 4 ist, wenn also der Grad der Gleichung $f(x) = 0$ den vierten übersteigt, so kann man in φ eine cyclische Substitution von fünf Buchstaben, z. B.

$$(x_1, x_2, x_3, x_4, x_5)$$

ausführen. Die Function F erleidet dadurch keine Veränderung, und man erhält

$$\varphi(x_2, x_3, x_4, x_5, x_1, \ldots) = \alpha\varphi(x_1, x_2, x_3, x_4, x_5, \ldots);$$

wird sodann beiderseits dieselbe Substitution wiederholt, so ergeben sich die Gleichungen

$$\varphi(x_3, x_4, x_5, x_1, x_2, \ldots) = \alpha\varphi(x_2, x_3, x_4, x_5, x_1, \ldots),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

deren Multiplication

$$\alpha^5 = 1$$

liefert. Diese Gleichung zieht aber, da α eine kubische Wurzel der Einheit ist,

$$\alpha = 1$$

nach sich. Wenn also der Grad der vorgelegten Gleichung grösser als 4 ist, so erleidet die Function φ, im Widerspruch mit unserer Voraussetzung, durch die cyclischen Substitutionen von drei Buchstaben keine Veränderung. Danach müssten alle in dem Ausdrucke der Wurzel einer allgemeinen Gleichung, deren Grad den vierten übersteigt, enthaltenen Wurzelgrössen rationalen Functionen der Wurzeln gleich sein, welche durch die cyclischen Substitutionen dreier Wurzeln keine Aenderung erleiden. Durch Einsetzung dieser Functionen in den Ausdruck von x_1 gelangt man dann zu einer Gleichung von der Form

$$x_1 = \psi(x_1, x_2, x_3, x_4, x_5, \ldots),$$

welche identisch bestehen muss. Das ist nun unmöglich; denn wenn man x_1, x_2, x_3 durch x_2, x_3, x_1 ersetzt, so bleibt das zweite Glied dieser Gleichung unverändert, während das erste offenbar eine Aenderung erleidet.

Die allgemeine Gleichung vom fünften oder von einem höheren Grade lässt sich also durch Wurzelgrössen nicht auflösen.

Der vorstehende Beweis zeigt zugleich, dass bei den Gleichungen dritten und vierten Grades zuerst eine Quadratwurzel, sodann eine Kubikwurzel auszuziehen ist. In der That zeigt sich dies in den Formeln, die wir im vorigen Kapitel hergeleitet haben.

Anmerkung. — Wie die allgemeine Gleichung fünften Grades mittels transcendenter Functionen gelöst werden kann, hat Hermite (Compt. rend. 1858) gezeigt.

Drittes Kapitel.

Abel'sche Gleichungen.

Irreductibele Gleichungen, bei denen zwei Wurzeln in einem solchen Zusammenhange stehen, dass die eine rational durch die andere ausgedrückt werden kann.

517. Nachdem wir gezeigt haben, dass es unmöglich ist, die allgemeinen Gleichungen, deren Grad den 4ten übersteigt, algebraisch zu lösen, würde es naturgemäss sein, die Gleichungen zu ermitteln, welche einer solchen Auflösung fähig sind. Bevor wir aber diese schwierige Aufgabe in Angriff nehmen, halten wir es für zweckmässig, eine bemerkenswerthe Klasse von Gleichungen eingehend zu behandeln, welche Kronecker Abel'sche Gleichungen genannt hat.

Die Gleichungen, zu welchen die Aufgabe führt, den Kreis in p gleiche Theile zu theilen, wo p eine Primzahl bezeichnet, sind immer durch Wurzelgrössen lösbar, und Gauss hat in seinen Disquisitiones arithmet. bewiesen, dass jede der Wurzelgrössen, aus denen der Ausdruck der Wurzeln zusammengesetzt ist, einen der Primfactoren von $p - 1$ zum Exponenten hat. Diese Gleichungen haben die Eigenschaft, dass jede Wurzel rational durch jede der übrigen ausgedrückt werden kann, und von dieser Bemerkung ausgehend hat Abel gezeigt, dass wenn zwei Wurzeln einer irreductibelen Gleichung in einem solchen Zusammenhange stehen, dass die eine rational durch die andere ausgedrückt werden kann, die Auflösung der Gleichung sich immer auf die Auflösung von Gleichungen niedrigerer Grade zurückführen lässt. Es giebt sogar Fälle, in denen die Gleichung algebraisch auflösbar ist. Im Besonderen tritt dies ein, wenn ihr Grad eine Primzahl ist.

Wir wollen diese Untersuchungen Abel's jetzt darlegen und seine Methode sodann auf die Gleichungen anwenden, von welchen die Theilung des Kreises in gleiche Theile abhängt, deren Anzahl eine Primzahl ist.

518. Es sei

$$(1). \qquad f(x) = 0$$

eine irreductibele Gleichung μ^{ten} Grades, und es werde vorausgesetzt, zwei Wurzeln derselben x' und x_1 seien durch die Gleichung

$$x' = \Theta x_1$$

mit einander verbunden, wo Θx eine rationale Function von x und den bekannten Grössen bezeichnet. Da x' Wurzel der Gleichung (1) ist, so hat man

$$f(\Theta x_1) = 0;$$

daraus geht hervor, dass x_1 die Gleichung

$$(2). \qquad f(\Theta x) = 0$$

befriedigt. Diese Gleichung (2) muss folglich (No. 100) alle Wurzeln von (1) zulassen; denn die Gleichung (1) ist irreductibel und $f(\Theta x)$ eine rationale Function. Mit andern Worten, wenn x irgend eine Wurzel der Gleichung (1) bezeichnet, so muss auch Θx eine Wurzel dieser Gleichung sein. Nun ist aber Θx_1 eine Wurzel von (1); folglich ist es auch $\Theta\Theta x_1$, ebenso $\Theta\Theta\Theta x_1$, und man erhält allgemein stets eine Wurzel von (1), man mag die mit Θ bezeichnete Operation an x_1 ausführen, so oft man will.

Wird der Kürze wegen

$$\Theta\Theta x_1 = \Theta^2 x_1\,,\ \Theta\Theta^2 x_1 = \Theta^3 x_1\,,\ \Theta\Theta^3 x_1 = \Theta^4 x_1\,,\ \ldots$$

gesetzt, so sind alle Terme der Reihe

$$(3). \qquad x_1\,,\ \Theta x_1\,,\ \Theta^2 x_1\,,\ \Theta^3 x_1\,,\ \ldots$$

Wurzeln der Gleichung (1). Die Reihe (3) enthält aber eine unendliche Menge von Termen, während die Gleichung (1) nur μ Wurzeln besitzt; es müssen daher einige der Grössen (3) unendlich oft wiederkehren.

Nehmen wir z. B. an, es sei

$$\Theta^{m+n} x_1 = \Theta^m x_1,$$

oder

$$\Theta^n(\Theta^m x_1) - \Theta^m x_1 = 0,$$

so hat die Gleichung

$$\Theta^n x - x = 0$$

die Wurzel $\Theta^m x_1$ mit (1) gemeinschaftlich; sie lässt daher alle Wurzeln von (1) zu, und man hat

$$\Theta^n x_1 - x_1 = 0,$$

oder

$$\Theta^n x_1 = x_1.$$

Daraus ergiebt sich

$$\Theta^{n+k} x_1 = \Theta^k x_1.$$

Wir sehen somit, dass die Terme der Reihe (3) vom n^{ten} Terme an unaufhörlich in derselben Reihenfolge wiederkehren, und dass diese Reihe (3) nur die n verschiedenen Wurzeln

$$(4). \qquad x_1\,, \Theta x_1\,, \Theta^2 x_1\,, \ldots, \Theta^{n-1} x_1$$

enthält.

Diese n Wurzeln sind wirklich von einander verschieden, wenn n ausdrückt, wie oft man an x_1 die mit Θ bezeichnete Operation vollziehen muss, um wieder den Werth x_1 zu erhalten.

Wenn $\mu = n$ ist, so enthält die Reihe (3) alle Wurzeln der Gleichung (1).

Wird $\mu > n$ vorausgesetzt, und ist x_2 eine Wurzel der Gleichung (1), welche sich in der Reihe (4) nicht vorfindet, so zeigt man mittels des oben angewandten Schlussverfahrens, dass die Grössen

$$(5). \qquad x_2\,, \Theta x_2\,, \Theta^2 x_2\,, \ldots, \Theta^{n-1} x_2\,, \ldots$$

sämmtlich gleichfalls Wurzeln von (1) sind. Wir behaupten nun, dass nur die n ersten Terme der Reihe (5), nämlich

$$(6). \qquad x_2\,, \Theta x_2\,, \Theta^2 x_2\,, \ldots, \Theta^{n-1} x_2$$

von einander verschieden sein können. Die Gleichung

$$\Theta^n x - x = 0$$

lässt nämlich die Wurzel x_1, folglich auch alle übrigen Wurzeln der Gleichung (1) zu, und man hat

$$\Theta^n x_2 = x_2,$$

mithin

$$\Theta^{n+k} x_2 = \Theta^k x_2.$$

Daher kehren auch die Terme der Reihe (5), vom n^{ten} Terme an, in derselben Reihenfolge unaufhörlich wieder, und die einzigen derselben, die von einander verschieden sein können, sind in der Reihe (6) enthalten.

Die Terme der Reihe (6) sind nun wirklich von einander und von den Grössen (4) verschieden.

In der That kann man nicht

$$\Theta^k x_2 = \Theta^i x_2$$

haben, wenn k und i kleiner als n sind; denn nach dem Lehrsatze der No. 100 würde daraus

$$\Theta^k x_1 = \Theta^i x_1$$

folgen, was nicht der Fall ist, weil die Grössen (4) von einander verschieden sind.

Ebenso kann nicht

$$\Theta^k x_2 = \Theta^i x_1$$

sein; denn wenn dies der Fall wäre, so müsste

$$\Theta^{n-k} \Theta^i x_1 = \Theta^{n-k} \Theta^k x_2,$$

oder

$$\Theta^{n-k+i} x_1 = \Theta^n x_2 = x_2,$$

folglich x_2, der Voraussetzung zuwider, ein Term der Reihe (4) sein.

Die Anzahl der in den Reihen (4) und (6) enthaltenen Wurzeln der Gleichung (1) ist $2n$; man hat daher entweder $\mu = 2n$, oder $\mu > 2n$.

Setzen wir $\mu > 2n$ voraus und bezeichnen eine Wurzel der Gleichung (1), welche sich in keiner der beiden Gruppen (4) und (6) vorfindet, mit x_3, so können wir eine dritte Gruppe von n Wurzeln

$$x_3, \Theta x_3, \Theta^2 x_3, \ldots, \Theta^{n-1} x_3$$

bilden, welche sämmtlich von einander und von den Grössen (4) und (6) verschieden sind; es muss daher entweder $\mu = 3n$, oder $\mu > 3n$ sein.

Durch Fortsetzung dieser Betrachtung erkennt man, dass die μ Wurzeln der Gleichung (1) in eine gewisse Anzahl m Gruppen vertheilt werden können, deren jede aus n Termen besteht, so dass

$$\mu = mn$$

ist. Die Wurzeln der Gleichung (1) sind dann

$$(7). \quad \begin{cases} x_1 \,,\ \Theta x_1 \,,\ \Theta^2 x_1 \,,\ \ldots \,,\ \Theta^{n-1} x_1 \,, \\ x_2 \,,\ \Theta x_2 \,,\ \Theta^2 x_2 \,,\ \ldots \,,\ \Theta^{n-1} x_2 \,, \\ x_3 \,,\ \Theta x_3 \,,\ \Theta^2 x_3 \,,\ \ldots \,,\ \Theta^{n-1} x_3 \,, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_m \,,\ \Theta x_m \,,\ \Theta^2 x_m \,,\ \ldots \,,\ \Theta^{n-1} x_m \,. \end{cases}$$

519. Betrachten wir die Gleichung n^{ten} Grades, deren Wurzeln die Terme einer dieser Gruppen, etwa der ersten sind. Diese Gleichung sei

$$(x - x_1)(x - \Theta x_1)(x - \Theta^2 x_1) \ldots (x - \Theta^{n-1} x_1) = 0$$

oder

$$(8). \quad x^n + A_1^{(1)} x^{n-1} + A_2^{(1)} x^{n-2} + \cdots + A_{n-1}^{(1)} x + A_n^{(1)} = 0.$$

Die Coefficienten

$$A_1^{(1)} \,,\ A_2^{(1)} \,,\ \ldots \,,\ A_n^{(1)}$$

sind rationale und symmetrische Functionen der Grössen

$$x_1 \,,\ \Theta x_1 \,,\ \Theta^2 x_1 \,,\ \ldots \,,\ \Theta^{n-1} x_1$$

und hängen, wie wir sehen werden, von nur einer Gleichung m^{ten} Grades ab.

Es sei nämlich y_1 irgendeine rationale und symmetrische Function der Grössen

$$(9). \quad x_1 \,,\ \Theta x_1 \,,\ \Theta^2 x_1 \,,\ \ldots \,,\ \Theta^{n-1} x_1 \,.$$

Da Θx_1, $\Theta^2 x_1$, u. s. w. rationale Functionen von x_1 sind, so ist dasselbe mit y_1 der Fall; wir setzen

$$y_1 = F(x_1),$$

wo also F eine rationale Function bezeichnet. Der Relation $\Theta^n x_1 = x_1$ wegen werden ausserdem die Grössen (9) sich nur gegen einander vertauschen, wenn man x_1 durch

$$\Theta x_1 \,,\ \Theta^2 x_1 \,,\ \ldots \,,\ \Theta^{n-1} x_1$$

ersetzt, und da die Function y_1 in Beziehung auf diese Grössen symmetrisch ist, so erleidet sie durch diese Vertauschungen keine Aenderung. Man hat daher

$$y_1 = F(x_1) = F(\Theta x_1) = F(\Theta^2 x_1) = \cdots = F(\Theta^{n-1} x_1).$$

Werden die Werthe, welche y_1 annimmt, wenn man x_1 der Reihe nach durch

$$x_2\,,\,x_3\,,\,\ldots\,,\,x_m$$

ersetzt, mit

$$y_2\,,\,y_3\,,\,\ldots\,,\,y_m$$

bezeichnet, so ist

$$\begin{aligned}
y_2 &= F(x_2) = F(\Theta x_2) = F(\Theta^2 x_2) = \cdots = F(\Theta^{n-1} x_2),\\
&\ldots\ldots\ldots\ldots\ldots\ldots,\\
y_m &= F(x_m) = F(\Theta x_m) = F(\Theta^2 x_m) = \cdots = F(\Theta^{n-1} x_m).
\end{aligned}$$

Es sei jetzt

$$(y - y_1)(y - y_2)\ldots(y - y_m) = 0$$

oder

$$(10).\qquad y^m + p_1 y^{m-1} + p_2 y^{m-2} + \cdots + p_{m-1} y + p_m = 0$$

die Gleichung, welche $y_1\,,\,y_2\,,\,\ldots\,,\,y_m$ zu Wurzeln hat. Wir behaupten, dass die Coefficienten $p_1\,,\,p_2$, u. s. w. dieser Gleichung sich rational durch diejenigen der vorgelegten Gleichung (1) ausdrücken lassen. Man hat nämlich für jeden Werth der ganzen Zahl λ

$$\begin{aligned}
y_1^\lambda &= \frac{1}{n}\left\{[F(x_1)]^\lambda + [F(\Theta x_1)]^\lambda + \cdots + [F(\Theta^{n-1} x_1)]^\lambda\right\},\\
y_2^\lambda &= \frac{1}{n}\left\{[F(x_2)]^\lambda + [F(\Theta x_2)]^\lambda + \cdots + [F(\Theta^{n-1} x_2)]^\lambda\right\},\\
&\ldots\ldots\ldots\ldots\ldots\ldots,\\
y_m^\lambda &= \frac{1}{n}\left\{[F(x_m)]^\lambda + [F(\Theta x_m)]^\lambda + \cdots + [F(\Theta^{n-1} x_m)]^\lambda\right\},
\end{aligned}$$

und durch Addition dieser Formeln ergiebt sich

$$y_1^\lambda + y_2^\lambda + \cdots + y_m^\lambda = \frac{1}{n}\sum [F(x)]^\lambda.$$

Das Zeichen $\sum$ des zweiten Gliedes erstreckt sich über alle Wurzeln der vorgelegten Gleichung. Dieses zweite Glied ist daher eine rationale und symmetrische Function aller Wurzeln. Daraus geht hervor, dass die Summen der gleichen Potenzen der Wurzeln von (10) rational durch die Coefficienten der vorgelegten Gleichung ausgedrückt werden können. Auf dieselbe Weise müssen sich daher auch, wie wir behauptet hatten, die Coefficienten $p_1\,,\,p_2$, u. s. w. ausdrücken lassen.

Die rationale und symmetrische Function y_1 der Grössen (9), die nach Belieben gewählt werden kann, hängt also direct von einer Gleichung m^{ten} Grades ab. Zudem sind

$$y_1\,,\,A_1^{(1)}\,,\,A_2^{(1)}\,,\,\ldots\,,\,A_n^{(1)}$$

ähnliche Functionen; denn man kann sie sämmtlich als rationale Functionen der einen Wurzel x_1 ansehen. Es lassen sich somit

$$A_1^{(1)}\,,\; A_2^{(1)}\,,\; \ldots\,,\; A_n^{(1)}$$

rational durch y_1 ausdrücken.

Wir sind so zu einer der wichtigsten Anwendungen der Theorie der ähnlichen Functionen geführt, die wir in dem fünften Kapitel des vierten Theils entwickelt haben. Da aber diese Theorie einigen Ausnahmefällen unterliegt, so dürfte es von Nutzen sein, Abel in die Einzelheiten der Berechnung der Coefficienten $A_1^{(1)}$, $A_2^{(1)}$, ... zu folgen.

Es bezeichne $\psi(x_1)$ irgendeinen dieser Coefficienten. ψ ist wie y_1 eine rationale und symmetrische Function der Grössen (9), die sich daher nicht ändern darf, wenn man x_1 durch

$$\Theta x_1\,,\; \Theta^2 x_1\,,\; \ldots\; \Theta^{n-1} x_1$$

ersetzt. Dasselbe ist mit der Function

$$y_1^\lambda \psi(x_1) \text{ oder } [F(x_1)]^\lambda \psi(x_1)$$

der Fall. Es ist also

$$y_1^\lambda \psi(x_1) = \frac{1}{n}\Big\{[F(x_1)]^\lambda \psi(x_1) + [F(\Theta x_1)]^\lambda \psi(\Theta x_1) + \cdots \\ + [F(\Theta^{n-1} x_1)]^\lambda \psi(\Theta^{n-1} x_1)\Big\}.$$

Wird hierin x_1 der Reihe nach durch $x_2, x_3, \ldots\, x_m$ ersetzt, so erhält man ähnliche Ausdrücke für $y_2^\lambda \psi(x_2)$, ..., $y_m^\lambda \psi(x_m)$, und wenn man

$$(11). \qquad t_\lambda = y_1^\lambda \psi(x_1) + y_2^\lambda \psi(x_2) + \cdots + y_m^\lambda \psi(x_m)$$

setzt, so folgt

$$t_\lambda = \frac{1}{n} \sum [F(x)]^\lambda \psi(x),$$

wo das Zeichen $\sum$ sich über alle Wurzeln der Gleichung (1) erstreckt. Man ersieht daraus, dass t_λ eine rationale und symmetrische Function der Wurzeln der Gleichung (1) ist, also rational durch die bekannten Grössen ausgedrückt werden kann.

Dies vorausgesetzt, liefert die Gleichung (11), wenn man darin λ die Werthe

$$0\,,\, 1\,,\, 2\,,\, 3\,,\, \ldots\,,\, (m-1)$$

annehmen lässt, die folgenden Gleichungen:

$$(12).\quad \begin{cases} \psi(x_1) + \psi(x_2) + \cdots + \psi(x_m) = t_0, \\ y_1\psi(x_1) + y_2\psi(x_2) + \cdots + y_m\psi(x_m) = t_1, \\ y_1^2\psi(x_1) + y_2^2\psi(x_2) + \cdots + y_m^2\psi(x_m) = t_2, \\ \dots\dots\dots\dots\dots\dots, \\ y_1^{m-1}\psi(x_1) + y_2^{m-1}\psi(x_2) + \cdots + y_m^{m-1}\psi(x_m) = t_{m-1}, \end{cases}$$

deren zweite Glieder als bekannt angesehen werden können.

Um den Werth von $\psi(x_1)$ zu erhalten, addiren wir die Gleichungen (12), nachdem wir sie beziehungsweise mit den unbestimmten Grössen

$$R_0\,,\ R_1\,,\ \dots,\ R_{m-2}\,,\ 1$$

multiplicirt haben, und machen der Kürze wegen

$$(13).\qquad \varphi(y) = y^{m-1} + R_{m-2}y^{m-2} + \cdots + R_1 y + R_0.$$

Es ergiebt sich

$$\varphi(y_1)\psi(x_1) + \varphi(y_2)\psi(x_2) + \cdots + \varphi(y_m)\psi(x_m)$$
$$= t_0 R_0 + t_1 R_1 + \cdots + t_{m-2}R_{m-2} + t_{m-1},$$

und daraus folgt, wenn die Factoren R_0, R_1, ... mittels der Bedingungen

$$\varphi(y_2) = 0\ ,\ \varphi(y_3) = 0\,,\ \dots,\ \varphi(y_m) = 0$$

bestimmt werden,

$$(14).\qquad \psi(x_1) = \frac{t_0R_0 + t_1R_1 + \cdots + t_{m-2}R_{m-2} + t_{m-1}}{\varphi(y_1)}.$$

Suchen wir jetzt die Werthe von R_0, R_1, u. s. w. Unserer Voraussetzung nach muss die Gleichung

$$\varphi(y) = 0$$

y_2, y_3, ..., y_m zu Wurzeln haben. Diese Wurzeln gehören aber auch der Gleichung (10) an, welche ausserdem die Wurzel y_1 zulässt. Man hat somit

$$(15).\quad \begin{cases} \varphi(y) = \dfrac{y^m + p_1y^{m-1} + p_2y^{m-2} + \cdots + p_{m-1}y + p_m}{y - y_1} \\ \quad = y^{m-1} \begin{array}{l} + p_1 \\ + y_1 \end{array} \Bigg| \, y^{m-2} \begin{array}{l} + p_2 \\ + p_1y_1 \\ + y_1^2 \end{array} \Bigg| \, y^{m-3} + \cdots + \begin{array}{l} p_{m-1} \\ + p_{m-2}y_1 \\ + \dots\dots \\ \dots\dots\dots \\ + p_1 y_1^{m-2} \\ + y_1^{m-1}. \end{array} \end{cases}$$

Vergleicht man die Werthe von $\varphi(y)$, welche die Gleichungen (13) und (15) liefern, so erhält man

$$(16).\quad \begin{cases} R_{m-2} = p_1 + y_1, \\ R_{m-3} = p_2 + p_1 y_1 + y_1^2, \\ \dots\dots\dots\dots\dots\dots, \\ R_1 \quad = p_{m-2} + p_{m-3} y_1 + \cdots + y_1^{m-2}, \\ R_0 \quad = p_{m-1} + p_{m-2} y_1 + \cdots + y_1^{m-1}. \end{cases}$$

Aus der Gleichung (15) folgt auch

$$\varphi(y_1) = m y_1^{m-1} + (m-1) p_1 y_1^{m-2} + \cdots + 2 p_{m-2} y_1 + p_{m-1},$$

und wenn der Kürze wegen

$$\begin{aligned} T_0 \quad &= t_0 p_{m-1} + t_1 p_{m-2} + \cdots + t_{m-2} p_1 + t_{m-1}, \\ T_1 \quad &= t_0 p_{m-2} + t_1 p_{m-3} + \cdots + t_{m-2}, \\ &\dots\dots\dots\dots\dots\dots, \\ T_{m-2} &= t_0 p_1 + t_1, \\ T_{m-1} &= t_0 \end{aligned}$$

gemacht wird, so erhält man für $\psi(x_1)$ folgenden Werth:

$$(17).\quad \psi(x_1) = \frac{T_{m-1} y_1^{m-1} + T_{m-2} y_1^{m-2} + \cdots + T_1 y_1 + T_0}{m y_1^{m-1} + (m-1) p_1 y_1^{m-2} + \cdots + 2 p_{m-2} y_1 + p_{m-1}}.$$

Diese Formel wird nur dann illusorisch, wenn der Nenner des zweiten Gliedes Null ist. Wir behaupten nun, dass man dies immer vermeiden könne. Der in Rede stehende Nenner ist nämlich gleich dem Produkte

$$(y_1 - y_2)(y_1 - y_3) \cdots (y_1 - y_m),$$

und damit dieses Null sei, muss einer der Factoren verschwinden, etwa

$$y_1 = y_k$$

sein. Dies vorausgesetzt, nehmen wir für y_1 die Function

$$y_1 = (\alpha - x_1)(\alpha - \Theta x_1)(\alpha - \Theta^2 x_1) \ldots (\alpha - \Theta^{n-1} x_1),$$

worin α unbestimmt ist. Die Gleichung $y_1 = y_k$ oder

$$(\alpha - x_1)(\alpha - \Theta x_1) \cdots = (\alpha - x_k)(\alpha - \Theta x_k) \ldots$$

kann für keinen Werth von α bestehen, wofern sie nicht eine Identität ist. Das ist unmöglich, da die Grössen x_k, Θx_k, ... von x_1, Θx_1, ... verschieden sind. Daraus folgt, dass wenn man y_1 in der eben angegebenen Weise wählt, die Gleichung (17) für $\psi(x_1)$ einen endlichen und bestimmten Werth liefert.

Die Coefficienten $A_1^{(1)}$, $A_2^{(1)}$, u. s. w. der Gleichung (8) können also rational durch ein und dieselbe Function y_1 ausgedrückt werden, deren Werth von einer Gleichung m^{ten} Grades abhängt, und wenn man y_1 der Reihe nach durch $y_2, y_3, \ldots, y_m$ ersetzt, so erhält man m Gleichungen n^{ten} Grades, deren Wurzeln beziehungsweise folgende sind:

$$\begin{array}{l} x_1\,,\ \Theta x_1\,,\ \ldots\,,\ \Theta^{n-1} x_1\,,\\ x_2\,,\ \Theta x_2\,,\ \ldots\,,\ \Theta^{n-1} x_2\,,\\ \ldots\ldots\ldots\ldots\ldots\\ x_m\,,\ \Theta x_m\,,\ \ldots\,,\ \Theta^{n-1} x_m. \end{array}$$

Die vorgelegte Gleichung kann danach in m Gleichungen n^{ten} Grades zerlegt werden, deren Coefficienten beziehungsweise rationale Functionen ein und derselben Wurzel einer Gleichung m^{ten} Grades sind.

Diese letzte Gleichung ist im Allgemeinen nicht algebraisch lösbar, wenn ihr Grad den vierten übersteigt. Dagegen lassen sich die Gleichung (8) und die übrigen ähnlichen Gleichungen stets algebraisch auflösen. Dies wollen wir jetzt nachweisen. Dabei setzen wir die Coefficienten $A_1^{(1)}$, $A_2^{(1)}$, ... als bekannt voraus. Unter dieser Voraussetzung führt unsere Untersuchung die Auflösung der vorgelegten Gleichung vom Grade $\mu = mn$ auf diejenige von m Gleichungen n^{ten} Grades zurück, welche die Eigenschaft haben, dass alle Wurzeln jeder derselben durch

$$x\,,\ \Theta x\,,\ \Theta^2 x\,,\ \ldots\,,\ \Theta^{n-1} x$$

dargestellt werden können.

Algebraische Auflösung der Gleichungen, deren sämmtliche Wurzeln durch x, Θx, $\Theta^2 x$, ..., $\Theta^{\mu-1} x$ dargestellt werden können. Θx ist eine rationale Function von x und den bekannten Grössen, für welche $\Theta^\mu x = x$ ist.

520. Es sei

$$f(x) = 0 \tag{1}$$

eine Gleichung μ^{ten} Grades, deren Wurzeln

$$x\,,\ \Theta x\,,\ \Theta^2 x\,,\ \ldots\,,\ \Theta^{\mu-1} x$$

sind; Θx bezeichnet eine rationale Function von x und den bekannten Grössen, für welche man

(2). $$\Theta^{\mu} x = x,$$

folglich

(3). $$\Theta^{\mu+k} x = \Theta^{k} x$$

hat.

Bezeichnen wir mit α irgend eine Wurzel der Gleichung

$$x^{\mu} = 1$$

und setzen mit Lagrange (No. 508)

(4). $$\psi(x) = (x + \alpha\Theta x + \alpha^2\Theta^2 x + \cdots + \alpha^{\mu-1}\Theta^{\mu-1} x)^{\mu},$$

so lässt sich zeigen, dass $\psi(x)$ rational durch die bekannten Grössen von $f(x)$ und Θx ausgedrückt werden kann.

Wird nämlich in der Gleichung (4) x durch $\Theta^m x$ ersetzt, so folgt

$$\psi(\Theta^m x) = (\Theta^m x + \alpha\Theta^{m+1} x + \alpha^2\Theta^{m+2} x + \cdots + \alpha^{\mu-1}\Theta^{m+\mu-1} x)^{\mu},$$

und mit Rücksicht auf die Gleichungen (2) und (3)

$$\psi(\Theta^m x) = (\Theta^m x + \alpha\Theta^{m+1} x + \cdots + \alpha^{\mu-m} x + \alpha^{\mu-m+1}\Theta x + \cdots + \alpha^{\mu-1}\Theta^{m-1} x)^{\mu}$$

$$(\alpha^{\mu-m} x + \alpha^{\mu-m+1}\Theta x + \cdots + \alpha^{\mu-1}\Theta^{m-1} x + \Theta^m x + \cdots + \alpha^{\mu-m-1}\Theta^{\mu-1} x)^{\mu}$$

$$(\alpha^{\mu-m})^{\mu}(x + \alpha\Theta x + \alpha^2\Theta^2 x + \cdots + \alpha^{\mu-1}\Theta^{\mu-1} x)^{\mu},$$

oder endlich, der Relation $\alpha^{\mu} = 1$ wegen,

$$\psi(\Theta^m x) = \psi(x).$$

Ertheilt man hierin m der Reihe nach die Werthe

$$0, 1, 2, \ldots, \mu - 1,$$

so ergiebt sich

$$\psi(x) = \psi(\Theta x) = \psi(\Theta^2 x) = \cdots = \psi(\Theta^{\mu-1} x),$$

folglich

$$\psi(x) = \frac{1}{\mu}[\psi(x) + \psi(\Theta x) + \cdots + \psi(\Theta^{\mu-1} x)].$$

Daraus geht hervor, dass ψx eine rationale und symmetrische Function aller Wurzeln der Gleichung (1) ist, also rational durch die Coefficienten dieser Gleichung ausgedrückt werden kann.

Setzen wir jetzt

$$\psi(x) = v,$$

so ist v als bekannt anzusehen, und man hat

$$x + \alpha\Theta x + \alpha^2\Theta^2 x + \cdots + \alpha^{\mu-1}\Theta^{\mu-1} x = \sqrt[\mu]{v}.$$

Bezeichnen

$$1\,,\ \alpha_1\,,\ \alpha_2\,,\ \ldots\,,\ \alpha_{\mu-1}$$

die μ Wurzeln der Gleichung

$$x^\mu = 1\,,$$

ferner

$$v_0\,,\ v_1\,,\ v_2\,,\ \ldots\,,\ v_{\mu-1}$$

die entsprechenden Werthe von v, so hat man

$$(5).\ \begin{cases} x + \Theta x + \Theta^2 x + \cdots\cdots + \Theta^{\mu-1}x = \sqrt[\mu]{v_0}\,, \\ x + \alpha_1\,\Theta x + \alpha_1^2\,\Theta^2 x + \cdots + \alpha_1^{\mu-1}\Theta^{\mu-1}x = \sqrt[\mu]{v_1}\,, \\ x + \alpha_2\,\Theta x + \alpha_2^2\,\Theta^2 x + \cdots + \alpha_2^{\mu-1}\Theta^{\mu-1}x = \sqrt[\mu]{v_2}\,, \\ \ldots\ldots\ldots\ldots\ldots\ldots\,, \\ \ldots\ldots\ldots\ldots\ldots\ldots\,, \\ x + \alpha_{\mu-1}\Theta x + \alpha_{\mu-1}^2\Theta^2 x + \cdots + \alpha_{\mu-1}^{\mu-1}\Theta^{\mu-1}x = \sqrt[\mu]{v_{\mu-1}}\,. \end{cases}$$

Die Grösse $\sqrt[\mu]{v_0}$ wird unmittelbar durch die Gleichung (1) gegeben; denn wenn man den Coefficienten, welchen $x^{\mu-1}$ in dieser Gleichung hat, mit A bezeichnet, so ist

$$\sqrt[\mu]{v_0} = -A.$$

Durch Addition der Gleichungen (5) ergiebt sich mit Rücksicht auf die bekannten Eigenschaften der Wurzeln α

$$(6).\qquad x = \frac{-A + \sqrt[\mu]{v_1} + \sqrt[\mu]{v_2} + \cdots + \sqrt[\mu]{v_{\mu-1}}}{\mu}\,,$$

und allgemein erhält man den Werth irgend einer Wurzel $\Theta^m x$, wenn man die Gleichungen (5) addirt, nachdem dieselben beziehungsweise mit

$$1\,,\ \alpha_1^{-m}\,,\ \alpha_2^{-m}\,,\ \alpha_3^{-m}\,,\ \ldots\,,\ \alpha_{\mu-1}^{-m}$$

multiplicirt worden sind. Es ergiebt sich auf diese Weise

$$(7).\quad \Theta^m x = \frac{-A + \alpha_1^{-m}\sqrt[\mu]{v_1} + \alpha_2^{-m}\sqrt[\mu]{v_2} + \cdots + \alpha_{\mu-1}^{-m}\sqrt[\mu]{v_{\mu-1}}}{\mu}\,.$$

Diese Formel liefert die Werthe von $\Theta x\,,\ \Theta^2 x\,,\ \ldots\,,\ \Theta^{\mu-1}x$, wenn man darin m die Werthe $1, 2, 3, \ldots, (\mu-1)$ annehmen lässt.

521. In (6) und in den Gleichungen, die man aus der Formel (7) herleitet, hat man jeder Wurzelgrösse

$$\sqrt[\mu]{v_1}, \sqrt[\mu]{v_2}, \ldots, \sqrt[\mu]{v_{\mu-1}}$$

immer denselben Werth zu ertheilen. Lässt man diesen Wurzelgrössen ihre volle Allgemeinheit, so sind die Gleichungen (6) und (7) nicht von einander verschieden, und (6) enthält den Ausdruck aller Wurzeln. Es tritt hier indess eine Schwierigkeit zu Tage. Die Gleichung (6) liefert nämlich für x einen Ausdruck, welcher $\mu^{\mu-1}$ Werthe hat, während die Gleichung (1) nur μ Wurzeln besitzt. Wir hatten aber schon Gelegenheit anzugeben, wie diese Unbestimmtheit beseitigt werden kann, und es ist leicht zu zeigen, dass wenn man den Werth einer Wurzelgrösse fixirt hat, dadurch auch die übrigen bestimmt sein werden.

Bezeichnet nämlich α eine primitive Wurzel der Gleichung

$$\alpha^\mu = 1,$$

und wird

$$\alpha_1 = \alpha \ , \ \alpha_2 = \alpha^2 \ , \ \alpha_3 = \alpha^3 \ , \ \ldots \ , \ \alpha_{\mu-1} = \alpha^{\mu-1}$$

gesetzt, so ist

$$\sqrt[\mu]{v_1} = x + \alpha \ \Theta x + \alpha^2 \Theta^2 x + \cdots + \alpha^{\mu-1} \Theta^{\mu-1} x,$$

$$\sqrt[\mu]{v_n} = x + \alpha^n \Theta x + \alpha^{2n} \Theta^2 x + \cdots + \alpha^{(\mu-1)n} \Theta^{\mu-1} x.$$

Verwandelt man x in $\Theta^m x$, so geht, wie aus der oben ausgeführten Rechnung erhellt, $\sqrt[\mu]{v_1}$ in $\alpha^{\mu-m} \sqrt[\mu]{v_1}$ über. Durch dieselbe Veränderung von x in $\Theta^m x$ wird $\sqrt[\mu]{v_n}$ mit $\alpha^{n(\mu-m)}$, also das Produkt

$$\sqrt[\mu]{v_n} \left(\sqrt[\mu]{v_1}\right)^{\mu-n}$$

mit $\alpha^{\mu(\mu-m)} = 1$ multiplicirt, d. h. dasselbe erleidet keine Aenderung. Setzt man daher

$$\sqrt[\mu]{v_n} \left(\sqrt[\mu]{v_1}\right)^{\mu-n} = \varphi(x),$$

so ist

$$\varphi(x) = \varphi(\Theta x) = \varphi(\Theta^2 x) = \cdots = \varphi(\Theta^{\mu-1} x),$$

folglich

$$\varphi(x) = \frac{1}{\mu}\left[\varphi(x) + \varphi(\Theta x) + \cdots + \varphi(\Theta^{\mu-1} x)\right].$$

$\varphi(x)$ ist mithin eine rationale und symmetrische Function der Wurzeln der Gleichung (1) und kann rational durch die bekann-

ten Grössen ausgedrückt werden. Wird der Werth dieser Function mit a_n bezeichnet, so hat man

$$\sqrt[\mu]{v_n}\left(\sqrt[\mu]{v_1}\right)^{\mu-n}=a_n,$$

oder

$$\sqrt[\mu]{v_n}=\frac{a_n}{v_1}\left(\sqrt[\mu]{v_1}\right)^n.$$

Auf diese Weise lässt sich jede der Wurzelgrössen $\sqrt[\mu]{v_2}$, $\sqrt[\mu]{v_3}$, u. s. w. rational durch $\sqrt[\mu]{v_1}$ ausdrücken, und die Gleichung (6) nimmt die Form an:

$$(8).\quad x=\frac{1}{\mu}\left[-A+\sqrt[\mu]{v_1}+\frac{a_2}{v_1}\left(\sqrt[\mu]{v_1}\right)^2+\frac{a_3}{v_1}\left(\sqrt[\mu]{v_1}\right)^3+\cdots+\frac{a_{\mu-1}}{v_1}\left(\sqrt[\mu]{v_1}\right)^{\mu-1}\right].$$

Dieser Ausdruck von x hat genau μ Werthe und stellt die μ Wurzeln der vorgelegten Gleichung dar.

Die vorstehende Entwicklung liefert folgenden Satz:

Lehrsatz I. — Wenn die μ Wurzeln irgend einer Gleichung durch

$$x,\ \Theta x,\ \Theta^2 x,\ \ldots,\ \Theta^{\mu-1}x$$

dargestellt werden können, wo Θx eine rationale Function von der Beschaffenheit ist, dass man $\Theta^\mu x=x$ hat, so ist die Gleichung immer durch Wurzelgrössen lösbar.

Durch Verbindung dieses Lehrsatzes mit den Ergebnissen der No. 519 erhält man einen zweiten Satz:

Lehrsatz II. — Wenn zwei Wurzeln einer irreductibelen Gleichung, deren Grad eine Primzahl ist, so beschaffen sind, dass die eine rational durch die andere ausgedrückt werden kann, so ist die Gleichung durch Wurzelgrössen lösbar.

Fall, in welchem die bekannten Grössen reell sind.

522. Wenn alle Coefficienten von f und von Θ reell sind, so findet ein wichtiger Satz statt, welchen Gauss zuerst für die Gleichungen bewiesen hat, von denen die Kreistheilung abhängt.

Wir haben oben

$$v_1=(x+\alpha\Theta x+\alpha^2\Theta^2 x+\cdots+\alpha^{\mu-1}\Theta^{\mu-1}x)^\mu$$

gesetzt und gezeigt, dass v_1 eine symmetrische Function der Wurzeln der Gleichung $f(x) = 0$ ist. v_1 ist folglich rational durch die Coefficienten von f und von Θ ausdrückbar, und wenn diese sämmtlich reell sind, so wird v_1 keine anderen complexen Grössen als diejenigen der Wurzel α enthalten. Ausserdem geht $v_{\mu-1}$ aus v_1 dadurch hervor, dass man α durch den conjugirten Ausdruck $\alpha^{\mu-1}$ ersetzt. Daraus folgt, dass v_1 und $v_{\mu-1}$ conjugirte complexe Grössen sind, und da wir v_1 kennen, so ist auch $v_{\mu-1}$ bekannt. Man kann daher

$$(1).\quad \begin{cases} v_1 = \varrho\,(\cos\omega + \sqrt{-1}\,\sin\omega), \\ v_{\mu-1} = \varrho\,(\cos\omega - \sqrt{-1}\,\sin\omega) \end{cases}$$

setzen. Auch ist allgemein

$$\left(\sqrt[\mu]{v_1}\right)^{\mu-n}\sqrt[\mu]{v_n} = a_n,$$

und für $n = \mu - 1$

$$(2).\quad \sqrt[\mu]{v_1}\,\sqrt[\mu]{v_{\mu-1}} = a_{\mu-1}.$$

$a_{\mu-1}$ ist rational durch die Coefficienten von f und von Θ ausdrückbar, kann also keine anderen als die in α sich vorfindenden complexen Grössen enthalten. Es liegt aber auf der Hand, dass $a_{\mu-1}$ sich nicht ändert, wenn man α durch den conjugirten Werth $\alpha^{\mu-1}$ ersetzt; $a_{\mu-1}$ ist somit reell.

Aus den Gleichungen (1) und (2) folgt

$$\varrho^2 = a^{\mu}_{\mu-1}$$

und, wenn a den numerischen Werth von $a_{\mu-1}$ bezeichnet,

$$\sqrt[\mu]{\varrho} = \sqrt{a}.$$

Die erste der Gleichungen (1) liefert dann folgenden Werth von $\sqrt[\mu]{v_1}$:

$$\sqrt[\mu]{v_1} = \sqrt{a}\,\left(\cos\frac{\omega + 2k\pi}{\mu} + \sqrt{-1}.\ \sin\frac{\omega + 2k\pi}{\mu}\right),$$

wo k eine ganze Zahl bezeichnet, und der durch die Gleichung (8) der No. 521 gegebene Ausdruck der Wurzeln x nimmt die bemerkenswerthe Form

$$x = \frac{1}{\mu}\Big\{ -A + \sqrt{a}\ \left(\cos\frac{\omega+2k\pi}{\mu} + \sqrt{-1}\ \sin\frac{\omega+2k\pi}{\mu}\right)$$

$$+ (f + g\sqrt{-1})\left[\cos\frac{2(\omega+2k\pi)}{\mu} + \sqrt{-1}\ \sin\frac{2(\omega+2k\pi)}{\mu}\right]$$

$$+ (f_1 + g_1\sqrt{-1})\left[\cos\frac{3(\omega+2k\pi)}{\mu} + \sqrt{-1}\ \sin\frac{3(\omega+2k\pi)}{\mu}\right]$$

$$+ (f_2 + g_2\sqrt{-1})\left[\cos\frac{4(\omega+2k\pi)}{\mu} + \sqrt{-1}\ \sin\frac{4(\omega+2k\pi)}{\mu}\right]$$

$$+ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \Big\}$$

an; darin sind a, f, g, f_1, g_1, u. s. w. rationale Functionen von $\cos\frac{2\pi}{\mu}$ und von $\sin\frac{2\pi}{\mu}$.

Die vorstehende Formel lehrt die μ Wurzeln von $f(x) = 0$ kennen, wenn man der ganzen Zahl k die μ Werthe

$$0, 1, 2, 3, \ldots, \mu - 1$$

ertheilt. Daraus ergiebt sich der folgende Satz:

Lehrsatz. — Um die vorgelegte Gleichung $f(x) = 0$ aufzulösen, genügt es:

1^0 den ganzen Kreisumfang in μ gleiche Theile zu theilen; 2^0 einen Winkel ω, den man construiren kann, in μ gleiche Theile zu theilen; 3^0 die Quadratwurzel aus einer einzigen Grösse a zu ziehen.

Anmerkung. — Da die Coefficienten von f und von Θ sämmtlich reell sind, so sind alle Wurzeln von $f(x) = 0$ reell, wenn dies mit einer einzigen der Fall ist. Bezeichnet nämlich x diese reelle Wurzel, so sind die übrigen Wurzeln

$$\Theta x, \Theta^2 x, \ldots, \Theta^{\mu-1} x.$$

Die Wurzeln der vorgelegten Gleichung sind daher entweder sämmtlich reell, oder sämmtlich complex.

Erste besondere Methode für die Auflösung der Abel'schen Gleichungen, deren Grad eine zusammengesetzte Zahl ist.

523. Die Methode, die wir soeben für die algebraische Auflösung der Abel'schen Gleichung μ^{ten} Grades

(1). $$f(x) = 0$$

dargelegt haben, lässt sich auf alle Fälle anwenden, μ mag eine Primzahl sein, oder nicht. Wenn aber μ eine zusammengesetzte Zahl ist, so kann man die Auflösung noch vereinfachen, wie jetzt gezeigt werden soll.

Es sei $\mu = mn$. Die Wurzeln der Gleichung (1), welche wieder

$$x\,,\ \Theta x\,,\ \Theta^2 x\,,\ \ldots,\ \Theta^{\mu-1} x$$

sind, lassen sich in m Gruppen

$$\begin{array}{lllll} x\,, & \Theta^m x\,, & \Theta^{2m} x\,, & \ldots, & \Theta^{(n-1)m} x\,, \\ \Theta x\,, & \Theta^{m+1} x\,, & \Theta^{2m+1} x\,, & \ldots, & \Theta^{(n-1)m+1} x\,, \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \Theta^{m-1} x\,, & \Theta^{2m-1} x\,, & \Theta^{3m-1} x\,, & \ldots, & \Theta^{nm-1} x \end{array}$$

vertheilen. Setzt man

$$x = x_1\,,\ \Theta x = x_2\,,\ \Theta^2 x = x_3\,,\ \ldots,\ \Theta^{m-1} x = x_m$$

und

$$\Theta^m x = \Theta_1 x\,,$$

so sind diese Gruppen folgende:

$$(2).\qquad \left\{\begin{array}{lllll} x_1\,, & \Theta_1 x_1\,, & \Theta_1{}^2 x_1\,, & \ldots, & \Theta_1^{n-1} x_1\,, \\ x_2\,, & \Theta_1 x_2\,, & \Theta_1{}^2 x_2\,, & \ldots, & \Theta_1^{n-1} x_2\,, \\ \cdot & \cdot & \cdot & \cdot & \cdot\,, \\ x_m\,, & \Theta_1 x_m\,, & \Theta_1{}^2 x_m\,, & \ldots, & \Theta_1^{n-1} x_m\,. \end{array}\right.$$

Wendet man daher auf die Gleichung (1) die in No. 519 auseinandergesetzte Methode an, so kann man (1) in m Gleichungen n^{ten} Grades zerlegen, welche beziehungsweise die Terme der verschiedenen Gruppen (2) zu Wurzeln haben, und deren Coefficienten rationale Functionen ein und derselben Wurzel einer Gleichung m^{ten} Grades

$$(3).\qquad \psi(y) = 0$$

sind. Diese Gleichung (3) habe die m Wurzeln

$$y_1\,,\ y_2\,,\ \ldots,\ y_m\,,$$

und es seien

$$(4).\qquad \varphi(x, y_1) = 0\,,\ \varphi(x, y_2) = 0\,,\ \ldots,\ \varphi(x, y_m) = 0$$

die m Gleichungen, welche zu Wurzeln beziehungsweise die Terme der ersten, der zweiten, ..., der letzten Gruppe (2) haben. Wir

behaupten, dass es zur Auflösung der Gleichung (1) genügt, eine Wurzel y der Gleichung (3) und sodann eine Wurzel x der entsprechenden Gleichung

$$(5).\qquad \varphi(x, y) = 0$$

zu kennen. Auf diese Weise erhält man nämlich eine erste Wurzel x der Gleichung (1), und die übrigen Wurzeln sind dann

$$\Theta x, \Theta^2 x, \ldots, \Theta^{\mu-1} x.$$

Da die vorgelegte Gleichung algebraisch lösbar ist, so ist es auch die Gleichung (3); denn y bezeichnet eine rationale Function von x. Ausserdem lässt sich beweisen, dass die Gleichung (3) dieselbe Eigenschaft wie die Gleichung (1) besitzt, also nach derselben Methode aufgelöst werden kann.

Die in der ersten Gruppe (2) enthaltenen Wurzeln der Gleichung (1) sind nämlich

$$(6).\qquad x, \Theta^m x, \Theta^{2m} x, \ldots, \Theta^{(n-1)m} x,$$

und y bezeichnet eine rationale und symmetrische Function dieser Wurzeln, d. h. eine rationale Function von x.

Setzen wir

$$y = \mathfrak{F}(x, \Theta^m x, \Theta^{2m} x, \ldots, \Theta^{(n-1)m} x) = F(x),$$

so sind die m Wurzeln $y_1, y_2, \ldots, y_m$ der Gleichung (3)

$$F(x), F(\Theta x), F(\Theta^2 x) \ldots, F(\Theta^{m-1} x),$$

und man hat

$$F(\Theta x) = \mathfrak{F}(\Theta x, \Theta\Theta^m x, \Theta\Theta^{2m} x, \ldots, \Theta\Theta^{(n-1)m} x).$$

$F(\Theta x)$ und $F(x)$ sind folglich rationale und symmetrische Functionen der Grössen (6), und man kann die eine rational durch die andere ausdrücken, wenn man sich der Methode der ähnlichen Functionen bedient, die wir uns in No. 519 in's Gedächtniss zurückriefen.

Es sei also

$$F(\Theta x) = \lambda F(x) = \lambda y.$$

Da λy eine rationale Function von y ist, so erhält man

$$\begin{aligned}
F(\Theta^2 x) &= \lambda F(\Theta x) &&= \lambda^2 y,\\
F(\Theta^3 x) &= \lambda F(\Theta^2 x) &&= \lambda^3 y,\\
&\ldots\ldots\ldots\ldots &&,\\
F(\Theta^{m-1} x) &= \lambda F(\Theta^{m-2} x) &&= \lambda^{m-1} y,
\end{aligned}$$

und daraus ist ersichtlich, dass die m Wurzeln der Gleichung (3) durch

$$y\ ,\ \lambda y\ ,\ \lambda^2 y\ ,\ \ldots\ ,\ \lambda^{m-1} y$$

dargestellt werden können, wo λ eine rationale Function von der Beschaffenheit bezeichnet, dass

$$\lambda^m y = y$$

ist.

Hat man die Gleichung (3) aufgelöst, so ist y bekannt, und da die n Wurzeln der Gleichung (5) durch

$$x\ ,\ \Theta_1 x\ ,\ \Theta_1{}^2 x\ ,\ \ldots\ ,\ \Theta_1^{n-1} x$$

dargestellt werden können, so lässt sich auf dieselbe die früher dargelegte Methode anwenden. Es ergiebt sich somit der Satz:

Hat man $\mu = mn$, so wird die Auflösung der Gleichung (1) zurückgeführt auf die Auflösung zweier Gleichungen, deren Grade beziehungsweise m, n sind, und welche dieselbe Eigenschaft wie die vorgelegte Gleichung besitzen.

Wenn n selbst wieder eine zusammengesetzte Zahl $m_1 n_1$ ist, so hat man auf dieselbe Weise die Auflösung der Gleichung (5) auf die einer Gleichung $m_1{}^{\text{ten}}$ Grades in z

(7). $$\psi_1 (z\ ,\ y) = 0$$

und einer Gleichung $n_1{}^{\text{ten}}$ Grades in x

(8). $$\varphi_1 (x\ ,\ y\ ,\ z) = 0$$

zurückzuführen.

In der Gleichung (7) gehört y zu den bekannten Grössen; dasselbe ist in der Gleichung (8) mit den Grössen y und z der Fall, und allgemein besteht der folgende Satz:

Lehrsatz. — Wenn $\mu = m_1 m_2 \ldots m_n$ ist, so lässt sich die Auflösung der Gleichung (1) auf diejenige von n Gleichungen zurückführen, welche beziehungsweise die Grade

$$m_1\ ,\ m_2\ ,\ \ldots\ ,\ m_n$$

haben. Alle diese Gleichungen haben dieselbe Eigenschaft, wie die vorgelegte Gleichung, und es genügt, eine einzige Wurzel jeder derselben zu kennen.

Zusatz I. — Wenn man μ in Primfactoren zerlegt und

$$\mu = \varepsilon_1^{p_1}\,\varepsilon_2^{p_2}\,\ldots\,\varepsilon_\omega^{p_\omega}$$

erhält, so lässt sich die Auflösung der vorgelegten Gleichung μ^{ten} Grades zurückführen auf die Auflösung von p_1 Gleichungen $\varepsilon_1^{\text{ten}}$, p_2 Gleichungen $\varepsilon_2^{\text{ten}}$, ..., p_ω Gleichungen $\varepsilon_\omega^{\text{ten}}$ Grades.

Zusatz II. — Jede Gleichung vom Grade 2^p, deren Wurzeln durch

$$x\,,\ \Theta x\,,\ \Theta^2 x\,,\ \ldots\,,\ \Theta^{2^p-1}x$$

dargestellt werden können, lässt sich durch Ausziehung von p Quadratwurzeln auflösen.

524. Beispiel. — Nehmen wir $\mu = 30$ an, so hat die Gleichung

$$f(x) = 0 \tag{1}$$

die Wurzeln

$$x\,,\ \Theta x\,,\ \Theta^2 x\,,\ \ldots\,,\ \Theta^{29} x.$$

Da $30 = 2 \times 15$ ist, so hat man für y eine rationale und symmetrische Function der fünfzehn Wurzeln

$$x\,,\ \Theta^2 x\,,\ \Theta^4 x\,,\ \ldots\,,\ \Theta^{28} x$$

zu nehmen. y hängt dann von einer Gleichung zweiten Grades

$$y^2 + Ay + B = 0 \tag{2}$$

ab, deren Coefficienten sich rational durch diejenigen der vorgelegten Gleichung ausdrücken lassen. Man könnte sodann die Gleichung 15ten Grades bilden, welche $x\,,\ \Theta^2 x\,,\ \ldots\,,\ \Theta^{28} x$ zu Wurzeln hat. Es ist aber unnütz, diese Rechnung auszuführen. Wir stellen diese Gleichung, wie früher, durch

$$\varphi(x\,,\ y) = 0$$

dar; darin bezeichnet y eine bekannte Grösse. Da $15 = 3 \times 5$ ist, so hat man für z eine rationale und symmetrische Function der fünf Wurzeln

$$x\,,\ \Theta^6 x\,,\ \Theta^{12} x\,,\ \Theta^{18} x\,,\ \Theta^{24} x$$

zu nehmen. z hängt dann von einer Gleichung dritten Grades

$$z^3 + Cz^2 + Dz + E = 0 \tag{3}$$

ab, deren Coefficienten rationale Functionen von y und den bekannten Grössen sind. Endlich hat man die Gleichung

$$x^5 + Fx^4 + Gx^3 + Hx^2 + Kx + L = 0 \tag{4}$$

zu bilden, welche die Wurzeln

$$x\,,\ \Theta^6 x\,,\ \Theta^{12} x\,,\ \Theta^{18} x\,,\ \Theta^{24} x$$

hat, und deren Coefficienten rationale Functionen von y und von z sind. Um nun die Gleichung (1) aufzulösen, genügt es, eine Wurzel der Gleichung (2), sodann eine Wurzel der Gleichung (3), endlich eine Wurzel der Gleichung (4) zu bestimmen.

Zweite Methode.

525. Wir kehren zum allgemeinen Falle zurück und nehmen an, es sei

$$\mu = m_1\, m_2 \ldots m_\omega.$$

Bezeichnen $n_1\,, n_2\,, \ldots, n_\omega$ beziehungsweise die Quotienten der Division von μ durch $m_1\,, m_2\,, \ldots, m_\omega$, so ist

$$\mu = m_1\, n_1 = m_2\, n_2 = m_3\, n_3 = \ldots = m_\omega\, n_\omega.$$

Dies vorausgesetzt, kann man nach dem Vorhergehenden die Auflösung der Gleichung

$$f(x) = 0$$

auf diejenige zweier Gleichungen zurückführen, und zwar auf folgende ω Weisen:

(1). $\varphi_1(x\,, y_1) = 0$, welche Gleichung die Wurzeln

$$x\,,\ \Theta^{m_1} x\,,\ \Theta^{2m_1} x\,, \ldots,\ \Theta^{(n_1-1)\,m_1} x$$

hat, und deren Coefficienten rationale Functionen einer Wurzel y_1 einer Gleichung $m_1{}^{\text{ten}}$ Grades $\psi_1(y_1) = 0$ sind.

(2). $\varphi_2(x\,, y_2) = 0$, welche Gleichung die Wurzeln

$$x\,,\ \Theta^{m_2} x\,,\ \Theta^{2m_2} x\,, \ldots,\ \Theta^{(n_2-1)\,m_2} x$$

hat, und deren Coefficienten rationale Functionen einer Wurzel y_2 einer Gleichung $m_2{}^{\text{ten}}$ Grades $\psi_2(y_2) = 0$ sind.

. . . .

(ω). $\varphi_\omega(x\,, y_\omega) = 0$, welche Gleichung die Wurzeln

$$x\,,\ \Theta^{m_\omega} x\,,\ \Theta^{2m_\omega} x\,, \ldots,\ \Theta^{(n_\omega-1)\,m_\omega} x$$

hat, und deren Coefficienten rationale Functionen einer Wurzel y_ω einer Gleichung $m_\omega{}^{\text{ten}}$ Grades $\psi_\omega(y_\omega) = 0$ sind.

Nehmen wir jetzt an, die Zahlen $m_1, m_2, \ldots, m_\omega$ seien prim zu einander, so haben die Gleichungen

$$\varphi_1(x, y_1) = 0, \varphi_2(x, y_2) = 0, \ldots, \varphi_\omega(x, y_\omega) = 0$$

nur die Wurzel x gemeinschaftlich. Man kann daher x rational durch die Coefficienten dieser Gleichungen, folglich rational durch $y_1, y_2, \ldots, y_\omega$ ausdrücken. Da diese letzten Grössen bekannt sind, so erhält man auf diese Weise eine der Wurzeln von (1), und daraus lassen sich die übrigen leicht herleiten.

Die Auflösung der Gleichung (1) ist somit darauf zurückgeführt, eine Wurzel jeder der Gleichungen

$$\psi_1(y_1) = 0, \psi_2(y_2) = 0, \ldots, \psi_\omega(y_\omega) = 0$$

zu ermitteln, welche beziehungsweise von den Graden

$$m_1, m_2, \ldots, m_\omega$$

sind. Diese Gleichungen haben ausserdem, wie oben gezeigt wurde, dieselbe Eigenschaft wie die vorgelegte Gleichung, lassen sich also nach derselben Methode behandeln. Will man, dass dieselben von einem möglichst niedrigen Grade seien, so muss man, wenn sich bei der Zerlegung der Zahl μ in ihre Primfactoren

$$\mu = \varepsilon_1^{p_1} \varepsilon_2^{p_2} \ldots \varepsilon_\omega^{p_\omega}$$

ergiebt,

$$m_1 = \varepsilon_1^{p_1}, m_2 = \varepsilon_2^{p_2}, \ldots, m_\omega = \varepsilon_\omega^{p_\omega}$$

nehmen. Was die Auflösung jeder der Gleichungen vom Grade ε^p

$$\psi(y) = 0$$

betrifft, so lässt sich dieselbe, wie wir bewiesen haben, auf diejenige von p Gleichungen ε^{ten} Grades zurückführen.

Irreductibele Gleichungen, bei denen zwei Wurzeln x und x' durch die lineare Relation

$$x' = \frac{ax + b}{a'x + b'}$$

verbunden sind, in welcher a, b, a', b' gegebene Constanten bezeichnen.

526. Es sei

(1). $$f(x) = 0$$

eine irreductibele Gleichung, und es werde vorausgesetzt, zwischen zweien ihrer Wurzeln x und x' bestehe die Relation

$$(2).\qquad x' = \frac{ax + b}{a'x + b'} = \Theta x,$$

in welcher a, b, a', b' gegebene Constanten sind. Die in der Reihe

$$x,\ \Theta x,\ \Theta^2 x,\ \Theta^3 x,\ \ldots$$

enthaltenen Grössen müssen Wurzeln der Gleichung (1) sein, und eine der Functionen Θx, $\Theta^2 x$, ... ist, wie wir wissen, gleich x. Wir nehmen an, es sei

$$(3).\qquad \Theta^\mu x = x.$$

Diese Gleichung besteht identisch, wenn man a, b, a', b' als commensurabel oder wenigstens als rationale Functionen der Grössen voraussetzt, die man als bekannt ansieht und von denen die Coefficienten der vorgelegten Gleichung rational abhängen. Man erhält folglich die in No. 451 hergeleiteten Formeln

$$(4).\qquad \begin{cases} b' = -\left(a - 2\cos\dfrac{\lambda\pi}{\mu}\right), \\[2ex] b = -\dfrac{a^2 - 2a\cos\dfrac{\lambda\pi}{\mu} + 1}{a'}, \end{cases}$$

in denen λ eine ganze Zahl bezeichnet, welche prim zu μ ist.

Wenn $\mu = 2$ ist, so erfordert die Bedingung (3) nur, dass man

$$a + b' = 0$$

habe. Ausserdem kann man in diesem Falle

$$ab' - ba' = \pm 1$$

voraussetzen, und erhält dann

$$(5).\qquad \begin{cases} b' = -a \\[1ex] b = -\dfrac{a^2 \pm 1}{a'}. \end{cases}$$

Wir bezeichnen den Grad der Gleichung (1) mit $n\mu$ und stellen ihre $n\mu$ Wurzeln durch

$$\begin{array}{lllll} x, & \Theta x, & \Theta^2 x, & \ldots, & \Theta^{\mu-1} x, \\ x_1, & \Theta x_1, & \Theta^2 x_1, & \ldots, & \Theta^{\mu-1} x_1, \\ x_2, & \Theta x_2, & \Theta^2 x_2, & \ldots, & \Theta^{\mu-1} x_2, \\ \cdot & \cdot & \cdot & \cdot & \cdot\quad, \\ x_{n-1}, & \Theta x_{n-1}, & \Theta^2 x_{n-1}, & \ldots, & \Theta^{\mu-1} x_{n-1} \end{array}$$

dar. Wird dann

$$x + \Theta x + \Theta^2 x + \cdots + \Theta^{\mu-1} x = y \tag{6}$$

gesetzt, so hängt y von einer Gleichung n^{ten} Grades

$$F(y) = 0 \tag{7}$$

ab, deren Coefficienten rationale Functionen der bekannten Grössen der Gleichung (1) und der Function Θ sind. Die Gleichung (7) kann algebraisch unlösbar sein; dagegen hängen die Grössen

$$x\,,\ \Theta x\,,\ \Theta^2 x\,,\ \ldots\,,\ \Theta^{\mu-1} x$$

von einer Gleichung μ^{ten} Grades ab, deren Coefficienten rationale Functionen von y sind, und welche sich, wie wir wissen, auflösen lässt. Diese Gleichung ist im vorliegenden Falle nichts Anderes als die Gleichung (6), und daraus erhellt, dass die vorgelegte Gleichung (1) durch Elimination von y aus den beiden Gleichungen (6) und (7) hervorgehen muss. Das erste Glied der zweiten Gleichung kann als ein beliebiges irreductibeles Polynom n^{ten} Grades angesehen werden.

Mit anderen Worten können die Gleichungen, die wir betrachten, dadurch erhalten werden, dass man eine gewisse Anzahl n Gleichungen von der Form

$$\begin{aligned}
x + \Theta x + \Theta^2 x + \cdots + \Theta^{\mu-1} x - y \quad &= 0,\\
x + \Theta x + \Theta^2 x + \cdots + \Theta^{\mu-1} x - y_1 \quad &= 0,\\
x + \Theta x + \Theta^2 x + \cdots + \Theta^{\mu-1} x - y_2 \quad &= 0,\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots &\cdots,\\
x + \Theta x + \Theta^2 x + \cdots + \Theta^{\mu-1} x - y_{n-1} &= 0
\end{aligned}$$

multiplicirt; darin bezeichnen $y, y_1, y_2, \ldots, y_{n-1}$ die n Wurzeln einer irreductibelen Gleichung, deren Coefficienten völlig willkürliche Grössen sind.

Es liegt auf der Hand, dass man statt der Gleichung (6) die folgende nehmen kann:

$$x \times \Theta x \times \Theta^2 x \times \cdots \times \Theta^{\mu-1} x = y.$$

Irreductibele Gleichungen mit numerischen Coefficienten, bei denen mehrere Wurzeln sich in Kettenbrüche entwickeln lassen, welche mit denselben Quotienten schliessen.

527. Wir haben in No. 26 die Form der Gleichungen zweiten Grades kennen gelernt, deren Wurzeln sich in Kettenbrüche

entwickeln lassen, welche in dieselben Quotienten auslaufen. Dieselbe Frage lösten wir sodann (No. 500) hinsichtlich der Gleichungen dritten Grades. Die vorhergehenden Betrachtungen setzen uns in den Stand, die folgende allgemeinere Aufgabe zu behandeln:

Welche irreductibelen Gleichungen besitzen die Eigenschaft, dass, wenn man ihre reellen Wurzeln nach der Methode von Lagrange in Kettenbrüche entwickelt, zwei oder mehrere dieser Kettenbrüche mit denselben Quotienten schliessen?

Damit zwei Wurzeln x' und x einer Gleichung in Kettenbrüche dieser Art entwickelt werden können, ist nach No. 16 erforderlich und hinreichend, dass man

$$x' = \frac{ax + b}{a'x + b'} = \Theta x$$

habe, wo a, b, a', b' positive oder negative, durch die Relation

$$ab' - ba' = \pm 1$$

verbundene ganze Zahlen sind. Damit ausserdem x und Θx zwei Wurzeln einer irreductibelen Gleichung darstellen können, muss man eine ganze Zahl μ angeben können, für welche identisch

$$\Theta^{\mu} x = x$$

ist. Wie wir gesehen haben, erfordert dies, wenn $\mu > 2$ ist, dass man

$$b' = -\left(a - 2\cos\frac{\lambda\pi}{\mu}\right),$$

$$b = -\frac{a^2 - 2a\cos\frac{\lambda\pi}{\mu} + 1}{a'}$$

habe; darin ist λ eine ganze Zahl und prim zu μ. Im Falle $\mu = 2$ hat man

$$b' = -a,$$

$$b = -\frac{a^2 \pm 1}{a'}.$$

Da nun a, b, a', b' ganze Zahlen sind, so muss $2\cos\frac{\lambda\pi}{\mu}$ eine ganze Zahl sein, und, wenn wir vom Falle $\mu = 2$ absehen, so ist dies nur möglich, wenn $\mu = 3$ ist. Daraus ersieht man, dass die in Rede stehende Eigenschaft sich nur bei den irreductibelen Gleichungen vorfinden kann, deren Grad die Form $2n$ oder die

Form $3n$ hat. Wir werden diese beiden Klassen von Gleichungen einzeln untersuchen.

Setzt man $\mu = 2$ voraus, so ist

$$\Theta x = \frac{ax - \frac{a^2 \pm 1}{a'}}{a'x - a}$$

und

$$\Theta^2 x = x;$$

a bezeichnet irgend eine ganze Zahl und a' einen Divisor von $a^2 \pm 1$. Nimmt man für $F(y)$ irgend ein irreductibeles Polynom n^{ten} Grades und eliminirt y aus den beiden Gleichungen

$$x + \Theta x = y\,,\ F(y) = 0\,,$$

oder

$$x^2 - yx + \left(\frac{ay}{a'} - \frac{a^2 \pm 1}{a'^2}\right) = 0\,,\ F(y) = 0,$$

so erhält man die allgemeine Form der Gleichungen vom Grade $2n$, welche die Eigenschaft besitzen, dass ihre $2n$ Wurzeln in n Gruppen von der Beschaffenheit zerfallen, dass die Kettenbrüche, welche die Wurzeln einer jeden aus zwei reellen Wurzeln bestehenden Gruppe darstellen, mit denselben Quotienten schliessen. Dieser Satz kann noch auf eine andere Weise ausgesprochen werden:

Es seien a irgend eine ganze Zahl, a' irgend ein Divisor von $a^2 + 1$, und y irgend eine commensurabele oder incommensurabele reelle Grösse. Dann lassen sich die beiden Wurzeln der Gleichung

$$x^2 - yx + \left(\frac{ay}{a'} - \frac{a^2 \pm 1}{a'^2}\right) = 0$$

in Kettenbrüche entwickeln, welche mit denselben Quotienten endigen. Es stimmt dies mit dem in No. 26 erhaltenen Resultate überein.

Wir nehmen jetzt $\mu = 3$ an. Macht man $\lambda = 2$ (der Fall $\lambda = 1$ ist mit demjenigen, in welchem $\lambda = 2$ ist, identisch, und man geht von dem einen zum anderen dadurch über, dass man die Zeichen von a und a' ändert), so ergiebt sich

$$\Theta x = \frac{ax - \frac{a^2 + a + 1}{a'}}{a'x - (a + 1)}\,,$$

$$\Theta^2 x = \frac{(a+1)\,x - \frac{a^2+a+1}{a'}}{a'x - a},$$

$$\Theta^3 x = x;$$

a ist irgend eine ganze Zahl und a' ein Divisor von $a^2 + a + 1$. Die Irrationale x mag beschaffen sein, wie sie wolle, die Kettenbrüche, welche

$$x\,,\;\Theta x\,,\;\Theta^2 x$$

darstellen, endigen mit denselben Quotienten. Wenn also $F(y)$ irgend ein irreductibeles Polynom n^{ten} Grades bezeichnet, und y aus den beiden Gleichungen

$$x + \Theta x + \Theta^2 x = y\,,\; F(y) = 0\,,$$

oder

$$x^3 - yx^2 + \left[\frac{(2a+1)\,y}{a'} - \frac{3\,(a^2+a+1)}{a'^2}\right] x$$
$$- \left[\frac{a\,(a+1)\,y}{a'^2} - \frac{(2a+1)\,(a^2+a+1)}{a'^3}\right] = 0\,,$$
$$F(y) = 0$$

eliminirt wird, so erhält man den allgemeinen Ausdruck der Gleichungen vom Grade $3n$, deren $3n$ Wurzeln sich in n Gruppen von der Beschaffenheit vertheilen lassen, dass die Kettenbrüche, welche die Wurzeln einer jeden aus drei reellen Wurzeln bestehenden Gruppe darstellen, mit denselben Quotienten schliessen.

Im Besonderen sieht man, dass die Gleichungen dritten Grades, denen diese Eigenschaft zukommt, in folgender allgemeinen Form enthalten sind:

$$x^3 - yx^2 + \left[\frac{(2a+1)\,y}{a'} - \frac{3\,(a^2+a+1)}{a'^2}\right] x$$
$$- \left[\frac{a\,(a+1)\,y}{a'^2} - \frac{(2a+1)\,(a^2+a+1)}{a'^3}\right] = 0\,;$$

darin bezeichnet a irgend eine ganze Zahl, a' irgend einen Divisor von $a^2 + a + 1$, und y irgend eine commensurabele oder incommensurabele Grösse. Dies Resultat stimmt mit dem in No. 500 erhaltenen überein.

528. Die Gleichungen dritten Grades, von welchen die Theilung des Kreises in 7 oder in 9 gleiche Theile abhängt, und die Gleichung vierten Grades, zu der man bei der Theilung des

Kreises in 15 gleiche Theile gelangt, besitzen die merkwürdige Eigenschaft, die wir im Vorhergehenden studirt haben.

Die Theilung des Kreises in 7 gleiche Theile führt zu der Gleichung

$$x^3 + x^2 - 2x - 1 = 0,$$

und wenn man die positive Wurzel mit x, die beiden negativen Wurzeln mit $-x_1$ und $-x_2$ bezeichnet, so ist

$$x_1 = \frac{1}{1+x}, \; x_2 = 1 + \frac{1}{x}.$$

Die Wurzel x liegt zwischen 1 und 2; man erhält folglich Resultate von der Form:

$$x = 1 + \cfrac{1}{\alpha + \cfrac{1}{\beta + \cdots}}, \qquad x_1 = \cfrac{1}{2 + \cfrac{1}{\alpha + \cfrac{1}{\beta + \cdots}}},$$

$$x_2 = 1 + \cfrac{1}{1 + \cfrac{1}{\alpha + \cfrac{1}{\beta + \cdots}}}$$

Die Theilung des Kreises in 9 gleiche Theile führt zu der Gleichung

$$x^3 - 3x + 1 = 0.$$

Wird die zwischen -1 und -2 enthaltene negative Wurzel mit $-x$ bezeichnet, und stellen x_1 und x_2 die beiden positiven Wurzeln dar, so ist

$$x_1 = \frac{1}{1+x}, \; x_2 = 1 + \frac{1}{x},$$

was zu denselben Resultaten führt, wie der vorige Fall.

Die Gleichung vierten Grades endlich, zu welcher die Theilung des Kreises in 15 gleiche Theile führt, ist

$$x^4 - x^3 - 4x^2 + 4x + 1 = 0.$$

Bezeichnet man die beiden positiven Wurzeln mit x und x_1, die beiden negativen mit $-x'$ und $-x_1'$, so hat man

$$x = \frac{x'+2}{x'+1} = 1 + \frac{1}{1+x'},$$

$$x_1 = \frac{x_1'+2}{x_1'+1} = 1 + \frac{1}{1+x_1'}.$$

Die eine der beiden Grössen x' und x_1' liegt zwischen 0 und 1,

die andere zwischen 1 und 2; man erhält daher Resultate von der Form:

$$x' = \cfrac{1}{\alpha + \cfrac{1}{\beta + \cdots}}, \qquad x = 1 + \cfrac{1}{1 + \cfrac{1}{\alpha + \cfrac{1}{\beta + \cdots}}},$$

$$x_1' = 1 + \cfrac{1}{\alpha' + \cfrac{1}{\beta' + \cdots}}, \qquad x_1 = 1 + \cfrac{1}{2 + \cfrac{1}{\alpha' + \cfrac{1}{\beta' + \cdots}}}.$$

Die Gleichung, die wir betrachten, ergiebt sich durch Elimination von y aus

$$x + \frac{x-2}{x-1} = y \,,\; y^2 - y - 1 = 0.$$

Gleichungen, deren sämmtliche Wurzeln rational durch eine von ihnen ausgedrückt werden können.

529. Wir haben früher einen ausgedehnten Fall der Gleichungen betrachtet, deren sämmtliche Wurzeln rational durch eine von ihnen ausgedrückt werden können. Es war dies der Fall, in welchem, wenn μ den Grad der vorgelegten Gleichung bezeichnet, die Wurzeln sich durch

$$x \,,\; \Theta x \,,\; \Theta^2 x \,,\; \ldots \,,\; \Theta^{\mu-1} x$$

darstellen lassen; sie sind dann durch Wurzelgrössen ausdrückbar.

Es giebt noch einen andern Fall, in welchem Gleichungen algebraisch lösbar sind. Abel hat nämlich folgenden Satz bewiesen:

Lehrsatz. — Es sei $\chi(x) = 0$ irgend eine algebraische Gleichung, deren sämmtliche Wurzeln rational durch eine von ihnen, die wir mit x bezeichnen wollen, ausgedrückt werden können. Sind Θx und $\Theta_1 x$ zwei beliebige andere Wurzeln der Gleichung, so ist dieselbe algebraisch lösbar, wenn man

$$\Theta\Theta_1 x = \Theta_1 \Theta x$$

hat.

Wenn die vorgelegte Gleichung

(1). $$\chi(x) = 0$$

nicht irreductibel ist, so sei

(2). $$f(x) = 0$$

die irreductibele Gleichung μ^{ten} Grades, von welcher die Wurzel x abhängt. Das Polynom $f(x)$ ist dann ein rationaler Divisor von $\chi(x)$.

Ist Θx eine von x verschiedene Wurzel der Gleichung (2), so können die Wurzeln dieser Gleichung durch

$$\begin{array}{lllll} x\ , & \Theta x\ , & \Theta^2 x\ , & \ldots\ , & \Theta^{n-1} x\ , \\ x_1\ , & \Theta x_1\ , & \Theta^2 x_1\ , & \ldots\ , & \Theta^{n-1} x_1\ , \\ \cdot & \cdot & \cdot & \cdot & \cdot\ , \\ x_{m-1}\ , & \Theta x_{m-1}\ , & \Theta^2 x_{m-1}\ , & \ldots\ , & \Theta^{n-1} x_{m-1} \end{array}$$

dargestellt werden. Man hat dann

$$\mu = mn,$$

und wenn

(3). $$x^n + A^{(1)} x^{n-1} + A^{(2)} x^{n-2} + \ldots + A^{(n-1)} x + A^{(n)} = 0$$

die Gleichung darstellt, welche die Wurzeln

$$x, \Theta x, \Theta^2 x, \ldots, \Theta^{n-1} x$$

hat, so sind die Coefficienten $A^{(1)}, A^{(2)}, \ldots, A^{(n)}$, wie wir gesehen haben, rational durch eine Grösse y ausdrückbar, die von einer Gleichung m^{ten} Grades

(4). $$y + P^{(1)} y^{m-1} + P^{(2)} y^{m-2} + \cdots + P^{(m-1)} y + P^{(m)} = 0$$

abhängt; die Coefficienten von (4) sind rationale Functionen der bekannten Grössen.

Die Gleichung (4) ist irreductibel. Wäre nämlich das Gegentheil der Fall, so würde y eine Wurzel einer irreductibelen Gleichung vom Grade $m' < m$

(5). $$\varphi(y) = 0$$

sein, und die Elimination von y aus den Gleichungen (3) und (5) würde zu einer Gleichung

$$\psi(x) = 0$$

führen, deren Grad $m'n < \mu$ wäre. Das ist aber unmöglich, da die Gleichung μ^{ten} Grades (2) der Voraussetzung nach irreductibel ist.

Dies vorausgesetzt, wird die Auflösung der Gleichung (2) auf die der Gleichungen (3) und (4) zurückgeführt. Wir wissen bereits, dass die Gleichung (3) lösbar ist, und wollen jetzt darthun, dass (4) dieselbe Eigenschaft wie die Gleichung (2) besitzt.

Die Grösse y ist eine beliebige rationale und symmetrische Function der Wurzeln $x, \Theta x, \ldots, \Theta^{n-1}x$, und wenn man die m Wurzeln von (4) mit

$$y, y_1, y_2, \ldots, y_{m-1}$$

bezeichnet, so kann man

$$\begin{array}{ll} y & = \mathfrak{F}(x, \Theta x, \Theta^2 x, \ldots, \Theta^{n-1}x), \\ y_1 & = \mathfrak{F}(x_1, \Theta x_1, \Theta^2 x_1, \ldots, \Theta^{n-1}x_1), \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ , \\ y_{m-1} & = \mathfrak{F}(x_{m-1}, \Theta x_{m-1}, \Theta^2 x_{m-1}, \ldots, \Theta^{n-1}x_{m-1}) \end{array}$$

setzen, wo $\mathfrak{F}$ eine rationale und symmetrische Function bezeichnet. Ausserdem sind $x_1, x_2, \ldots, x_{m-1}$ der Voraussetzung nach rationale Functionen der Wurzel x. Macht man also

$$x_1 = \Theta_1 x, x_2 = \Theta_2 x, \ldots, x_{m-1} = \Theta_{m-1} x,$$

so erhält man für die Werthe $1, 2, 3, \ldots, m-1$ des Index i

$$y_i = \mathfrak{F}(\Theta_i x, \Theta\Theta_i x, \Theta^2\Theta_i x, \ldots, \Theta^{n-1}\Theta_i x).$$

Endlich sind, dem Ausspruche des Satzes zufolge, die Functionen Θ und Θ_i von der Beschaffenheit, dass man

$$\Theta\Theta_i x = \Theta_i \Theta x$$

hat. Daraus ergiebt sich

$$\Theta^j \Theta_i x = \Theta^{j-1}\Theta_i\Theta x = \Theta^{j-2}\Theta_i\Theta^2 x = \ldots = \Theta_i\Theta^j x,$$

und folglich kann man

$$y_i = \mathfrak{F}(\Theta_i x, \Theta_i\Theta x, \Theta_i\Theta^2 x, \ldots, \Theta_i\Theta^{n-1} x)$$

schreiben, woraus ersichtlich ist, dass y_i eine rationale und symmetrische Function der Wurzeln

$$x; \Theta x, \Theta^2 x, \ldots, \Theta^{n-1} x$$

ist. Dann sind aber (No. 519) $y_1, y_2, \ldots, y_{m-1}$ rational durch y ausdrückbar.

Es seien jetzt λy und $\lambda_1 y$ irgend zwei von y verschiedene Wurzeln der Gleichung (4), so kann man

$$(6).\qquad \begin{cases} y = F(x), \\ \lambda y = F(\Theta_i x), \\ \lambda_1 y = F(\Theta_j x) \end{cases}$$

setzen, und daraus folgt

$$\lambda\, F(x) = F(\Theta_i x),$$
$$\lambda_1 F(x) = F(\Theta_j x).$$

Nun ist x Wurzel einer irreductibelen Gleichung. Die vorstehenden Gleichungen bleiben also bestehen, wenn man x in der ersten durch $\Theta_j x$ und in der zweiten durch $\Theta_i x$ ersetzt; es ist daher

$$\lambda\, F(\Theta_j x) = F(\Theta_i\, \Theta_j x),$$
$$\lambda_1 F(\Theta_i x) = F(\Theta_j\, \Theta_i x),$$

folglich, da $\Theta_i\, \Theta_j\, x = \Theta_j\, \Theta_i x$ ist,

$$\lambda\, F(\Theta_j x) = \lambda_1\, F(\Theta_i x).$$

Die Gleichungen (6) gestatten es, der letzten Formel die Form

$$\lambda \lambda_1 y = \lambda_1 \lambda y$$

zu ertheilen, woraus hervorgeht, dass die Gleichung (4) dieselbe Eigenschaft wie die Gleichung (1) hat.

Man kann somit durch wiederholte Anwendung desselben Verfahrens die Auflösung der vorgelegten Gleichung auf die mehrerer Gleichungen zurückführen, welche sämmtlich algebraisch auflösbar sind, und deren Grade den Grad μ der Gleichung (2) zum Produkt haben.

Zusatz. — Wenn die Gleichung $f(x) = 0$ die im eben bewiesenen Lehrsatze angegebene Eigenschaft besitzt, und wenn sich bei der Zerlegung ihres Grades μ in Primfactoren

$$\mu = \varepsilon_1^{p_1}\, \varepsilon_2^{p_2} \ldots \varepsilon_\omega^{p_\omega}$$

ergiebt, so kann die Auflösung von $f(x) = 0$ zurückgeführt werden auf die Auflösung von p_1 Gleichungen $\varepsilon_1{}^{\text{ten}}$, p_2 Gleichungen $\varepsilon_2{}^{\text{ten}}$, ..., p_ω Gleichungen $\varepsilon_\omega{}^{\text{ten}}$ Grades. Alle diese Gleichungen haben rationale Coefficienten und sind algebraisch lösbar.

Algebraische Auflösung der binomischen Gleichungen.

530. Die binomische Gleichung

$$(1).\qquad z^m - A = 0$$

reducirt sich auf

$$(2). \qquad x^m - 1 = 0,$$

wenn man $z = x\sqrt[m]{A}$ setzt, und wir haben im 5ten Kapitel des 1ten Theils gesehen, dass die Aufsuchung der Wurzeln von (2), wenn m eine zusammengesetzte Zahl ist, sich auf die Auflösung von binomischen Gleichungen zurückführen lässt, deren Grade Primzahlen sind.

Wir nehmen daher an, der Exponent m sei eine Primzahl. Die Gleichung (2) lässt die Wurzel 1 zu, durch deren Unterdrückung man

$$(3). \qquad x^{m-1} + x^{m-2} + x^{m-3} + \cdots + x^2 + x + 1 = 0$$

erhält, welche Gleichung, wie wir in No. 110 bewiesen haben, irreductibel ist.

Die Gleichung (3) gehört zu der Klasse von Gleichungen, die wir Abel'sche genannt haben, und ihre Wurzeln können folglich durch algebraische Functionen ausgedrückt werden, in denen die Wurzelgrössen die Primfactoren von $m - 1$ zu Exponenten haben. Ist nämlich r eine primitive Wurzel von (3), so hat diese Gleichung die Wurzeln

$$r\,,\, r^2\,,\, r^3\,,\, \ldots\,,\, r^{m-1}.$$

Ausserdem hat man

$$r^m = 1,$$

und wenn a eine primitive Wurzel der Primzahl m bezeichnet, so sind die Potenzen

$$a^0\,,\, a^1\,,\, a^2\,,\, a^3\,,\, \ldots\,,\, a^{m-2}$$

abgesehen von der Reihenfolge beziehungsweise den Zahlen

$$1\,,\, 2\,,\, 3\,,\, \ldots\,,\, m-1$$

nach dem Modul m congruent. Die Wurzeln der Gleichung (3) können folglich durch

$$(4). \qquad r\,,\, r^a\,,\, r^{a^2}\,,\, r^{a^3}\,,\, \ldots\,,\, r^{a^{m-2}}$$

dargestellt werden, so dass jede derselben dadurch erhalten wird, dass man die vorhergehende auf die $a$te Potenz erhebt. Dasselbe ist, der Relation

$$a^{m-1} \equiv 1 \pmod{m}$$

wegen, noch der Fall, wenn man diese Wurzeln cyclisch ordnet und der Reihe nach jede als die erste ansieht.

Bezeichnet also x irgend eine der Wurzeln (4), und macht man

$$x^a = \Theta x,$$

so werden die in Rede stehenden $m-1$ Wurzeln durch

$$x\,,\ \Theta x\,,\ \Theta^2 x\,,\ \ldots\,,\ \Theta^{m-2} x$$

dargestellt, und man hat

$$\Theta^{m-1} x = x.$$

Auf diese Eigenschaft hat Gauss seine Auflösungsmethode der Gleichung (3) gegründet, welche Methode später von Abel in der dargelegten Weise verallgemeinert ist.

Man kann auf die Gleichung (2) die Methode der No. 520 anwenden und erhält dadurch folgenden Ausdruck der Wurzeln:

$$x = \frac{-A + \sqrt[m-1]{v_1} + \sqrt[m-1]{v_2} + \cdots + \sqrt[m-1]{v_{m-2}}}{m-1},$$

in welchem keine anderen Irrationale, als die Wurzeln der Gleichung

$$x^{m-1} = 1$$

enthalten sind.

Endlich kann man noch, da die Gleichung (3) reciprok ist, damit beginnen, ihren Grad zu erniedrigen. Man erhält dann eine Gleichung vom Grade $\frac{m-1}{2}$, deren sämmtliche Wurzeln reell sind, und welche gleichfalls zu den Abel'schen Gleichungen gehört. Dies wollen wir jetzt entwickeln.

Algebraische Auflösung der Gleichungen, von welchen die Theilung des Kreises in gleiche Theile abhängt, deren Anzahl eine Primzahl ist.

531. Die Aufgabe, den Kreisumfang in eine beliebige Anzahl m gleicher Theile zu theilen, lässt sich auf die Auflösung der binomischen Gleichung

(1). $$z^m - 1 = 0$$

zurückführen; denn macht man

$$\frac{2\pi}{m} = a,$$

so ergeben sich die m Wurzeln von (1), wenn man in der Formel

$$z = \cos ka + \sqrt{-1} \sin ka$$

k die m Werthe

$$0, 1, 2, 3, \ldots, (m-1)$$

ertheilt. Man kennt also $\cos ka$ und $\sin ka$, sobald die binomische Gleichung (1) algebraisch aufgelöst ist.

Ist m eine ungerade Zahl $2\mu + 1$, so folgt, wenn die Gleichung (1) durch $z - 1$ dividirt und darauf

$$z + \frac{1}{z} = x$$

gesetzt wird,

$$(2). \quad \left\{ \begin{array}{l} x^\mu + x^{\mu-1} - (\mu-1)\, x^{\mu-2} - (\mu-2)\, x^{\mu-3} \\ \quad + \frac{(\mu-2)(\mu-3)}{1 \cdot 2} x^{\mu-4} + \frac{(\mu-3)(\mu-4)}{1 \cdot 2} x^{\mu-5} - \ldots = 0. \end{array} \right.$$

Dies ist die Gleichung, von welcher die Theilung des Kreises in $2\mu + 1$ gleiche Theile direkt abhängt. Ihre μ Wurzeln werden durch die Formel

$$x = 2 \cos \frac{2k\pi}{2\mu + 1} = 2 \cos ka$$

dargestellt, in welcher man k die μ Werthe

$$1, 2, 3, \ldots, \mu,$$

oder Werthe zu geben hat, welche von den genannten nur durch Vielfache von $2\mu + 1$ verschieden sind.

Wir haben uns in der vorigen Nummer in's Gedächtniss zurückgerufen, dass, wenn m oder $2\mu + 1$ eine zusammengesetzte Zahl ist, die Auflösung der Gleichung (1) auf die Auflösung anderer Gleichungen von derselben Form zurückgeführt werden kann, deren Grade die in m aufgehenden Primzahlen oder Potenzen von Primzahlen sind. Dasselbe gilt dann von der Gleichung (2), und man kann sich darauf beschränken, den Fall zu betrachten, in welchem $m = 2\mu + 1$ eine Primzahl, oder eine Potenz einer Primzahl ist. Wenn m eine Primzahl ist, so erfordert die Theilung des Kreises in m gleiche Theile nur die Auflösung mehrerer Gleichungen, welche beziehungsweise die gleichen oder ungleichen Primfactoren von $m - 1$ zu Graden haben. Ist dagegen m eine Potenz p^i einer Primzahl p, so erfordert die Theilung des Kreises in m gleiche Theile die Theilung in p gleiche

Theile und sodann die Auflösung von $i-1$ Gleichungen p^{ten} Grades. Jede dieser $i-1$ Gleichungen p^{ten} Grades ist algebraisch lösbar. Dies ergiebt sich aus der Moivre'schen Formel und ebenso aus den im ersten Theile angestellten Betrachtungen.

Ausserdem ist zu bemerken, dass die Gleichung (2) für alle Werthe von μ zur Klasse der Gleichungen gehört, mit denen wir uns in No. 529 beschäftigt haben. Denn, wenn

$$x = 2 \cos a\ ,\ \Theta x = 2 \cos ia\ ,\ \Theta_1 x = 2 \cos ja$$

gemacht wird, so ist offenbar

$$\Theta\Theta_1 x = \Theta_1 \Theta x = 2 \cos ija.$$

532. Es sei $2\mu + 1$ eine Primzahl, und n eine primitive Wurzel dieser Zahl; dann behaupten wir, dass

$$(3).\qquad 2 \cos a\ ,\ 2 \cos na\ ,\ 2 \cos n^2 a\ ,\ \ldots\ ,\ 2 \cos n^{\mu-1} a$$

die μ Wurzeln der Gleichung (2) sind. Da es auf der Hand liegt, dass jede dieser μ Grössen (3) der Gleichung (2) genügt, so haben wir nur die Verschiedenheit derselben nachzuweisen.

Gesetzt, man hätte

$$2 \cos n^p a = 2 \cos n^q a$$

und $p < \mu$, $q < \mu$, so müsste

$$n^p a \pm n^q a = 2\lambda\pi$$

sein, wo λ eine ganze Zahl bezeichnet, und da $a = \dfrac{2\pi}{2\mu + 1}$ ist, so müsste

$$\frac{n^q (n^{p-q} \pm 1)}{2\mu + 1}$$

eine ganze Zahl sein. Nun ist aber $2\mu + 1$ eine Primzahl und n kleiner als $2\mu + 1$. Folglich müsste $2\mu + 1$ in eine der beiden Zahlen $n^{p-q} + 1$, $n^{p-q} - 1$, also auch in beider Produkt

$$n^{2p-2q} - 1$$

aufgehen. Das ist unmöglich, da da $2p - 2q < 2\mu$ ist, und n eine primitive Wurzel von $2\mu + 1$ bezeichnet. Die Grössen (3) sind daher die sämmtlichen Wurzeln der Gleichung (2).

Macht man jetzt

$$x = 2 \cos a\ ,\ \Theta x = 2 \cos na,$$

so ergiebt sich

$$\Theta^2 x = 2 \cos n^2 a\ ,\ \Theta^3 x = 2 \cos n^3 a\ ,\ \ldots,\ \Theta^{\mu-1} x = 2 \cos n^{\mu-1} a,$$

und die Wurzeln der Gleichung (2) können durch

$$x\,,\ \Theta x\,,\ \Theta^2 x\,,\ \ldots\,,\ \Theta^{\mu-1} x$$

dargestellt werden. Ausserdem hat man $\Theta^{\mu} x = x$; denn da n eine primitive Wurzel von $2\mu + 1$ bezeichnet, so ist $n^{\mu} \equiv -1$ $(mod.\ 2\mu + 1)$. Endlich ist Θx eine rationale Function von x; denn cos na lässt sich rational durch cos a ausdrücken. Wir sehen somit, dass die Gleichung (2) zu den Abel'schen Gleichungen gehört und deshalb nach den oben mitgetheilten Methoden behandelt werden kann.

Die rationale Function Θx hat hier den Werth (No. 109)

$$\Theta x = x^n - n x^{n-2} + \frac{n(n-3)}{1\,.\,2} x^{n-4} - \frac{n(n-4)(n-5)}{1\,.\,2\,.\,3} x^{n-6} + \cdots.$$

Wendet man auf die Gleichung (2) die Lehrsätze an, die wir in No. 522 und No. 523 hergeleitet haben, so ergiebt sich:

1⁰. Wenn $\mu = m_1\, m_2 \ldots m_\omega$ ist, so kann man den Kreis in $2\mu + 1$ gleiche Theile theilen mittels ω Gleichungen, deren Grade beziehungsweise $m_1, m_2, \ldots, m_\omega$ sind. Sind die Zahlen $m_1, m_2, \ldots, m_\omega$ prim zu einander, so haben diese Gleichungen rationale Coefficienten.

2⁰. Wenn $\mu = 2^\omega$ ist, so kann man den Kreis durch Ausziehung von ω Quadratwurzeln in $2\mu + 1$ gleiche Theile theilen. Mit andern Worten, wenn $2\mu + 1$ eine Primzahl und $\mu = 2^\omega$ ist, so lässt sich die Theilung des Kreises in $2\mu + 1$ gleiche Theile mit Zirkel und Lineal ausführen.

3⁰. Um den Kreis in $2\mu + 1$ gleiche Theile zu theilen, genügt es, den ganzen Kreis in 2μ gleiche Theile zu theilen, darauf einen Bogen, den man construiren kann, in 2μ gleiche Theile zu theilen und die Quadratwurzel aus einer einzigen Grösse zu ziehen.

533. Der letzte Satz ist von Gauss gefunden, der auch gezeigt hat, dass die Grösse, deren Quadratwurzel man zu berechnen hat, einfach die ganze Zahl $2\mu + 1$ ist. Dies beweist Abel auf folgende Weise:

Die in Rede stehende Grösse, die wir mit ϱ bezeichnen wollen, ist (No. 522) der numerische Werth des Produktes

$$(x + \alpha\, \Theta x + \alpha^2\, \Theta^2 x + \cdots + \alpha^{\mu-1}\, \Theta^{\mu-1} x)$$
$$\times\, (x + \alpha^{\mu-1}\, \Theta x + \alpha^{\mu-2}\, \Theta^2 x + \cdots + \alpha\, \Theta^{\mu-1} x),$$

wo

$$\alpha = \cos\frac{2\pi}{\mu} + \sqrt{-1}\,\sin\frac{2\pi}{\mu}$$

ist. Man hat daher

$$\pm\varrho = 4\,(\cos a + \alpha\cos na + \alpha^2\cos n^2a + \cdots + \alpha^{\mu-1}\cos n^{\mu-1}a)$$
$$\times\,(\cos a + \alpha^{\mu-1}\cos na + \alpha^{\mu-2}\cos n^2a + \cdots + \alpha\cos n^{\mu-1}a).$$

Die Entwicklung dieses Produktes liefert ein Resultat von der Form

$$\pm\varrho = t_0 + t_1\alpha + t_2\alpha^2 + \cdots + t_{\mu-1}\,\alpha^{\mu-1},$$

und man erhält leicht

$$t_m = 4\,(\cos a\cos n^m a + \cos na\cos n^{m+1}a + \cdots + \cos n^{\mu-1-m}a\cos n^{\mu-1}a)$$
$$+ 4\,(\cos n^{\mu-m}a\cos a + \cos n^{\mu-m+1}a\cos na + \cdots + \cos n^{\mu-1}a\cos n^{m-1}a).$$

Mittels der Formel

$$\cos n^p a\cos n^{m+p}a = \tfrac{1}{2}\cos(n^{m+p}a + n^p a) + \tfrac{1}{2}\cos(n^{m+p}a - n^p a),$$

kann man t_m die Form

$$t_m = 2\begin{bmatrix}\cos(n^m+1)\,a + \cos(n^m+1)\,na + \cos(n^m+1)\,n^2a + \cdots \\ + \cos(n^m+1)\,n^{\mu-1}a\end{bmatrix}$$
$$+ 2\begin{bmatrix}\cos(n^m-1)\,a + \cos(n^m-1)\,na + \cos(n^m-1)\,n^2a + \cdots \\ + \cos(n^m-1)\,n^{\mu-1}a\end{bmatrix},$$

oder, wenn

$$(n^m+1)\,a = a',\quad (n^m-1)\,a = a''$$

gemacht wird, die Form

$$t_m = 2\cos a' + \Theta\,2\cos a' + \Theta^2\,2\cos a' + \cdots + \Theta^{\mu-1}\,2\cos a'$$
$$+ 2\cos a'' + \Theta\,2\cos a'' + \Theta^2\,2\cos a'' + \cdots + \Theta^{\mu-1}\,2\cos a''$$

geben.

Dies vorausgesetzt, nehmen wir zunächst an, m sei von Null verschieden. $2\cos a'$ und $2\cos a''$ sind Wurzeln der Gleichung (2); folglich ist

$$2\cos a' = \Theta^\delta x,\quad 2\cos a'' = \Theta^\varepsilon x,$$

und man hat daher

$$t_m = (\Theta^\delta x + \Theta^{\delta+1}x + \cdots + \Theta^{\mu-1}x + x + \Theta x + \cdots + \Theta^{\delta-1}x)$$
$$+ (\Theta^\varepsilon x + \Theta^{\varepsilon+1}x + \cdots + \Theta^{\mu-1}x + x + \Theta x + \cdots + \Theta^{\varepsilon-1}x),$$

oder

$$t_m = 2\,(x + \Theta x + \Theta^2 x + \cdots + \Theta^{\mu-1}x).$$

Daraus geht hervor, dass t_m doppelt so gross als die Summe -1 der Wurzeln der Gleichung (2) ist, d. h. es ist

$$t_m = -2.$$

Wir setzen jetzt $m = 0$ voraus; dann ergiebt sich

$$t_0 = 2(\cos 2a + \cos 2na + \cos 2n^2a + \cdots + \cos 2n^{\mu-1}a) + 2\mu.$$

Nun ist $2\cos 2a$ eine Wurzel der Gleichung (2). Macht man daher

$$2\cos 2a = \Theta^\delta x,$$

so folgt

$$t_0 = (\Theta^\delta x + \Theta^{\delta+1}x + \cdots + \Theta^{\mu-1}x + x + \Theta x + \cdots + \Theta^{\delta-1}x) + 2\mu,$$

mithin

$$t_0 = 2\mu - 1.$$

Danach hat $\pm \varrho$ den Werth

$$\pm \varrho = 2\mu - 1 - 2(\alpha + \alpha^2 + \cdots + \alpha^{\mu-1}).$$

Ausserdem ist

$$\alpha + \alpha^2 + \cdots + \alpha^{\mu-1} = -1,$$

und wir erhalten somit

$$\pm \varrho = 2\mu + 1,$$

w. z. b. w.

Theilung des Kreises in 17 gleiche Theile.

534. Macht man $2\mu + 1 = 17$ oder $\mu = 8$, so geht die Gleichung (2) der vorigen Nummer über in

(1). $x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 - 10x^3 - 10x^2 - 4x + 1 = 0,$

und ihre Wurzeln, welche in der Formel

$$x = 2\cos\frac{2k\pi}{17}$$

enthalten sind, können durch

(2). $x,\ \Theta x,\ \Theta^2 x,\ \Theta^3 x,\ \Theta^4 x,\ \Theta^5 x,\ \Theta^6 x,\ \Theta^7 x$

dargestellt werden. Die kleinste primitive Wurzel von 17 ist 3 (No. 316), und die nach 17 genommenen Reste der Potenzen

$$3^0,\ 3^1,\ 3^2,\ 3^3,\ 3^4,\ 3^5,\ 3^6,\ 3^7$$

sind

$$1,\ 3,\ 9,\ 10,\ 13,\ 5,\ 15,\ 11.$$

Setzt man daher der Kürze wegen

$$a = \frac{2\pi}{17},$$

so sind die Grössen (2)

$$2 \cos a\ ,\ 2 \cos 3a\ ,\ 2 \cos 9a\ ,\ 2 \cos 10a,$$
$$2 \cos 13a\ ,\ 2 \cos 5a\ ,\ 2 \cos 15a\ ,\ 2 \cos 11a,$$

oder, der Relation $\cos(17-m)\,a = \cos ma$ wegen,

$$2 \cos a\ ,\ 2 \cos 3a\ ,\ 2 \cos 8a\ ,\ 2 \cos 7a,$$
$$2 \cos 4a,\ 2 \cos 5a\ ,\ 2 \cos 2a\ ,\ 2 \cos 6a.$$

Um die allgemeine Methode anzuwenden, hat man zunächst eine rationale und symmetrische Function y der Grössen

$$2 \cos a\ ,\ 2 \cos 8a\ ,\ 2 \cos 4a\ ,\ 2 \cos 2a$$

zu berechnen. Wir setzen daher

$$y = 2 \cos a + 2 \cos 8a + 2 \cos 4a + 2 \cos 2a.$$

y hängt dann von einer Gleichung zweiten Grades ab, welche die Wurzeln

(3). $$y = 2 \cos a + 2 \cos 8a + 2 \cos 4a + 2 \cos 2a,$$

(4). $$y_1 = 2 \cos 3a + 2 \cos 7a + 2 \cos 5a + 2 \cos 6a$$

hat. Diese Gleichung lässt sich sehr leicht ermitteln. Der Gleichung (1) wegen ist nämlich

(5). $$y + y_1 = -1.$$

Wenn man ferner y mit y_1 multiplicirt, die Produkte der Cosinus mittels bekannter Formeln in Summen verwandelt und sich der Identität

$$\cos(17-m)\,a = \cos ma$$

bedient, so erhält man

$$yy_1 = 4\,(2\cos a + 2\cos 2a + 2\cos 3a + 2\cos 4a + 2\cos 5a + 2\cos 6a + 2\cos 7a + 2\cos 8a),$$

und mit Rücksicht auf (1)

(6). $$yy_1 = -4.$$

Die Gleichung in y ist somit

(7). $$y^2 + y - 4 = 0,$$

und man kann ihre Wurzeln y, y_1 als bekannt ansehen.

Die Grössen

$$2 \cos a\ ,\ 2 \cos 8a\ ,\ 2 \cos 4a\ ,\ 2 \cos 2a$$

sind jetzt die Wurzeln einer Gleichung vierten Grades, deren Coefficienten rationale Functionen von y sind, und welche wir ebenso behandeln wollen, wie wir die vorgelegte Gleichung behandelten. Zunächst müssen wir der allgemeinen Methode gemäss eine rationale und symmetrische Function z der Grössen

$$2 \cos a \,,\; 2 \cos 4a$$

suchen. Wir setzen daher

$$z = 2 \cos a + 2 \cos 4a.$$

Die Gleichung in z ist vom zweiten Grade und hat die Wurzeln

(8). $$z = 2 \cos a + 2 \cos 4a,$$

(9). $$z_1 = 2 \cos 8a + 2 \cos 2a.$$

Nun ist

(10). $$z + z_1 = y,$$

und wenn man z mit z_1 multiplicirt, so ergiebt sich, nachdem die Produkte der Cosinus durch Summen ersetzt sind,

$$zz_1 = (2 \cos a + 2 \cos 2a + 2 \cos 3a + 2 \cos 4a \\ + 2 \cos 5a + 2 \cos 6a + 2 \cos 7a + 2 \cos 8a),$$

oder, weil die Wurzeln der Gleichung (1) die Summe -1 haben,

(11). $$zz_1 = -1.$$

Die Gleichung in z ist also

(12). $$z^2 - yz - 1 = 0.$$

Endlich haben wir noch die Gleichung zweiten Grades zu bilden, deren Wurzeln

$$2 \cos a \,,\; 2 \cos 4a$$

sind, und deren Coefficienten rational durch y und z ausgedrückt werden können. Man kann hier jedoch die Anwendung der allgemeinen Methode vereinfachen.

Wir betrachten die Gleichung vierten Grades, deren Wurzeln

$$2 \cos 3a \,,\; 2 \cos 7a \,,\; 2 \cos 5a ,\; 2 \cos 6a$$

die Summe y_1 haben, und verfahren ebenso, wie wir hinsichtlich der Gleichung verfuhren, deren Wurzeln die Summe y haben. Wir bilden also eine Gleichung zweiten Grades, deren Wurzeln

(13). $$u = 2 \cos 3a + 2 \cos 5a,$$

(14). $$u_1 = 2 \cos 7a + 2 \cos 6a$$

sind, und es ergiebt sich auf dem oben dargelegten Wege

(15). $$u + u_1 = y_1,$$

(16). $$uu_1 = -1.$$

Die Gleichung in u ist also

17. $$u^2 - y_1 u - 1 = 0,$$

so dass die Grössen u und u_1, ebenso wie z und z_1 bekannt sind.

Dies vorausgesetzt, machen wir

(18). $$x = 2 \cos a,$$

(19). $$x_1 = 2 \cos 4a.$$

Dann ist zunächst

(20). $$x + x_1 = z,$$

sodann

$$xx_1 = 4 \cos a \cos 4a = 2 \cos 3a + 2 \cos 5a,$$

oder

(21). $$xx_1 = u.$$

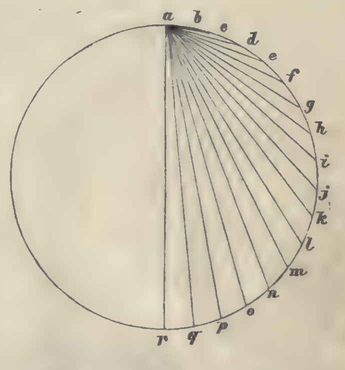
Danach sind x und x_1 Wurzeln der Gleichung

(22). $$x^2 - zx + u = 0.$$

Auf diese Weise ist die Auflösung der Gleichung (1) auf die der quadratischen Gleichungen (7), (12), (17) und (22) zurückgeführt, die Aufgabe somit gelöst. Wir wollen jetzt aus der vorstehenden Entwicklung eine geometrische Construction zu entnehmen suchen, mittels welcher der Kreis in 17 gleiche Theile getheilt werden könne.

Geometrische Construction.

535. Wenn man sich in den Elementen der Geometrie die Aufgabe stellt, ein regelmässiges Dreieck oder ein regelmässiges Fünfeck in einen Kreis zu beschreiben, so zeichnet man zunächst ein regelmässiges Sechseck oder ein regelmässiges Zehneck. Ebenso werden wir hier damit beginnen, ein regelmässiges Polygon von 34 Seiten zu construiren; daraus ergiebt sich dann sofort das regelmässige Siebenzehneck.



Es sei ein Halbkreis durch die Punkte $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r$ in 17 gleiche Theile getheilt. Die Sehne ab ist die Seite des eingeschriebenen regelmässigen Polygons von 34 Seiten, und die Sehnen ad, af, ah, aj

al, *an*, *ap*, welche Diagonalen dieses Polygons sind, sind die Seiten der sternförmigen regelmässigen Polygone von 34 Seiten, die man in den Kreis beschreiben kann.

Nimmt man den Radius als Längeneinheit an und macht, wie früher,

$$a = \frac{2\pi}{17},$$

so ergiebt sich

$$\begin{aligned}
ab &= 2 \sin \frac{\pi}{34} = + 2 \cos 4a, \\
ad &= 2 \sin \frac{3\pi}{34} = - 2 \cos 5a, \\
af &= 2 \sin \frac{5\pi}{34} = + 2 \cos 3a, \\
ah &= 2 \sin \frac{7\pi}{34} = - 2 \cos 6a, \\
aj &= 2 \sin \frac{9\pi}{34} = + 2 \cos 2a, \\
al &= 2 \sin \frac{11\pi}{34} = - 2 \cos 7a, \\
an &= 2 \sin \frac{13\pi}{34} = + 2 \cos a, \\
ap &= 2 \sin \frac{15\pi}{34} = - 2 \cos 8a.
\end{aligned}$$

Wir behalten alle Bezeichnungen der vorigen Nummer bei. Die Gleichungen (3) und (4) liefern

$$\begin{aligned}
y &= an - ap + ab + aj, \\
y_1 &= af - al - ad - ah.
\end{aligned}$$

Wie man sieht, ist y_1 negativ; denn man hat $af < al$. Da nun $yy_1 = -1$ ist, so muss y positiv sein. Macht man daher $y_1 = -y'$, so gehen die Gleichungen (5) und (6) über in

$$\begin{aligned}
y' - y &= 1, \\
yy' &= 4.
\end{aligned}$$

Die Gleichungen (8) und (9) liefern

$$\begin{aligned}
z &= an + ab, \\
z_1 &= - ap + aj.
\end{aligned}$$

z_1 ist negativ, da $ap > aj$ ist, und z ist positiv. Macht man $z_1 = -z'$, so gehen die Gleichungen (10) und (11) über in

$$\begin{aligned}
z - z' &= y, \\
zz' &= 1.
\end{aligned}$$

Ebenso liefern die Gleichungen (13) und (14)

$$u = af - ad,$$
$$u_1 = -al - ah;$$

u_1 ist somit negativ, u positiv. Macht man $u_1 = -u'$, so erhält man aus den Gleichungen (15) und (16)

$$u' - u = y',$$
$$uu' = 1.$$

Endlich liefern die Gleichungen (18) und (19)

$$x = an,$$
$$x_1 = ab,$$

so dass jede der Grössen x, x_1 positiv ist, und die Gleichungen (20) und (21) ihre Form

$$x + x_1 = z,$$
$$xx_1 = u$$

behalten.

Die Seite unseres Polygons von 34 Seiten ist x_1, und um dieselbe zu construiren, genügt es, wie man sieht,

1⁰ zwei Gerade y und y' von der Beschaffenheit zu construiren, dass

$$y' - y = 1, \quad yy' = 4$$

ist;

2⁰ vier Gerade z, z', u, u' von der Beschaffenheit zu construiren, dass

$$z - z' = y, \quad zz' = 1,$$
$$u' - u = y', \quad uu' = 1$$

ist;

3⁰ zwei Gerade x und x_1 von der Beschaffenheit zu construiren, dass

$$x + x_1 = z, \quad xx_1 = u$$

ist.

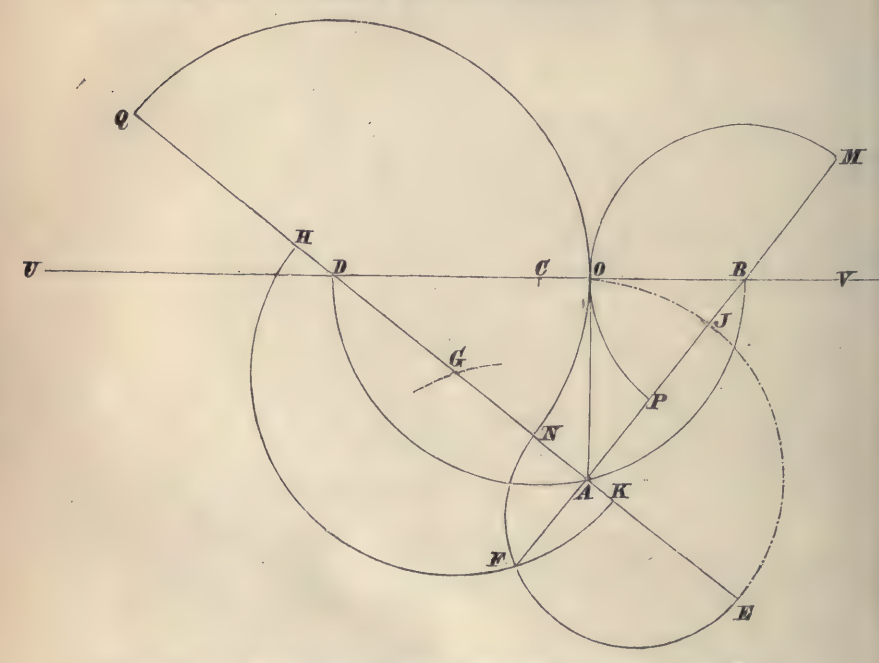
Construction. — 1⁰. In einem Punkte O einer beliebigen Geraden UV errichten wir eine Senkrechte OA, welche gleich dem Radius des Kreises, d. h. gleich der Einheit ist. Darauf machen wir $OC = \frac{1}{4}$ und beschreiben von C als Mittelpunkt aus mit dem Radius CA einen Kreis, welcher die Gerade UV in B und D schneidet. Dann hat man

$$OB = \tfrac{1}{2}\, y, \quad OD = \tfrac{1}{2}\, y';$$

denn es ist

$$2\,OD - 2\,OB = 4\,OC = 1 \text{ und } 2\,OD \times 2\,OB = 4\,\overline{OA}^2 = 4.$$

2⁰. Wir verbinden A mit B und schlagen von B als Mittelpunkt aus mit dem Radius BO einen Halbkreis, welcher die Linie



AB und deren Verlängerung in M und P schneidet; dann ist

$$AM = z\ ,\ AP = z',$$

da

$$AM - AP = PM = 2\,OB = y \text{ und } AM\,.\,AP = \overline{AO}^2 = 1$$

ist.

Ebenso verbinden wir A mit D und beschreiben von D als Mittelpunkt aus mit dem Radius OD einen Halbkreis, welcher die Linie AD und deren Verlängerung in N und Q schneidet; dann hat man

$$AN = u\ ,\ AQ = u',$$

da

$$AQ - AN = NQ = 2\,OD = y' \text{ und } AN\,.\,AQ = \overline{AO}^2 = 1$$

ist.

3⁰. Wir tragen AO auf der Verlängerung von AD ab, so dass $AE = AO$ ist, und beschreiben über NE als Durchmesser einen Halbkreis, welcher AB in F schneidet. Darauf beschreiben wir

vom Punkte F als Mittelpunkt aus mit dem Radius $AJ = \frac{AM}{2}$ einen Kreisbogen, welcher AD in G schneidet. Mit demselben Radius schlagen wir endlich von G als Mittelpunkt aus einen Kreisbogen, der AD in H und K schneidet. Dann ist

$$x_1 = AK \ , \ x = AH;$$

denn man hat

$$AK + AH = 2\,GF = 2\,AJ = AM = z$$

und

$$AK \,.\, AH = \overline{AF}^2 = AN \,.\, AE = AN \,.\, AO = u.$$

Die Seite des dem Kreise vom Radius OA eingeschriebenen regelmässigen Polygons von 34 Seiten ist daher gleich AK.

Ueber eine bemerkenswerthe Eigenschaft der Function $\frac{x^p - 1}{x - 1}$, in welcher p eine Primzahl ist.

536. Es sei p eine ungerade Primzahl, und es werde

$$X = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

gesetzt. Bezeichnet a eine primitive Wurzel von p und r eine Wurzel der Gleichung

(1). $$X = 0,$$

so sind

$$r^a \ , \ r^{a^2} \ , \ r^{a^3} \ , \ \ldots \ , \ r^{a^{p-1}}$$

die Wurzeln von (1), und es ist

$$a^{p-1} \equiv 1 \ (mod.\ p) \text{ und } r^{a^{p-1}} = r.$$

Macht man

$$y_1 = r^{a^2} + r^{a^4} + r^{a^6} + \cdots + r^{a^{p-1}},$$
$$y_2 = r^{a} + r^{a^3} + r^{a^5} + \cdots + r^{a^{p-2}},$$

so sind die Grössen y_1 und y_2 (No. 523) die Wurzeln einer Gleichung zweiten Grades mit commensurabelen Coefficienten, und die Gleichung (1) lässt sich in zwei andere Gleichungen zerlegen, deren jede vom Grade $\frac{p-1}{2}$ ist, und deren Coefficienten rationale Functionen von y_1 oder von y_2 sind. Wir wollen diese Zerlegung jetzt näher in's Auge fassen.

Erstens stellen wir uns die Aufgabe, die Gleichung in y zu bilden, welche y_1 und y_2 zu Wurzeln hat. Man hat zunächst

(2). $$y_1 + y_2 = -1,$$

da $y_1 + y_2$ die Summe aller Wurzeln der Gleichung (1) ausdrückt. Ferner ist, da die symmetrischen Functionen von y_1 und von y_2 sich nicht ändern, wenn man r in r^a, oder in r^{a^2}, oder u. s. w. verwandelt,

$$y_1^2 + y_2^2 = \frac{1}{\left(\frac{p-1}{2}\right)} \sum (x^{a^2} + x^{a^4} + x^{a^6} + \cdots + x^{a^{p-1}})^2,$$

wo das Zeichen Σ sich über alle Wurzeln x der Gleichung (1) erstreckt.

Nun ist

$$(x^{a^2} + x^{a^4} + \cdots + x^{a^{p-1}})^2 = \Sigma x^{a^{2m}+a^{2n}},$$

wo Σ sich über alle Werthe $1, 2, 3, \ldots, \frac{p-1}{2}$ der ganzen Zahlen m, n erstreckt. Bezeichnet daher $S(\mu)$ die Summe der μ^{ten} Potenzen der Wurzeln von (1), so hat man

$$y_1^2 + y_2^2 = \frac{1}{\left(\frac{p-1}{2}\right)} \Sigma S(a^{2m} + a^{2n}).$$

Das Zeichen Σ erstreckt sich über alle Werthe $1, 2, 3, \ldots, \frac{p-1}{2}$ der ganzen Zahlen m, n und umfasst folglich $\left(\frac{p-1}{2}\right)^2$ Terme. Da a eine primitive Wurzel von p ist, so ist

$$a^{\frac{p-1}{2}} + 1 \equiv 0 \ (mod.\ p),$$

und keine Potenz von a, deren Exponent kleiner als $\frac{p-1}{2}$ ist, kann nach dem Modul p congruent -1 sein. Danach ist die Summe

$$a^{2m} + a^{2n},$$

wenn p von der Form $4i + 1$ ist, nur für die folgenden $2i = \frac{p-1}{2}$ Systeme simultaner Werthe von m und n durch p theilbar:

$$\begin{array}{lllllllll} m = & 1, & 2, & 3, \ldots, & i, & i+1, & i+2, & \ldots, & 2i, \\ n = & i+1, & i+2, & i+3, \ldots, & 2i, & 1, & 2, & \ldots, & i. \end{array}$$

Wenn p die Form $4i + 3$ hat, so ist keiner der Werthe, welche die Summe

$$a^{2m} + a^{2n}$$

annimmt, durch p theilbar.

Nach No. 106 ist die Summe $S(\mu)$ gleich $p-1$, oder gleich -1, jenachdem μ durch p theilbar ist, oder nicht. Wenn also p die Form $4i+1$ hat, so ist die Grösse

$$\Sigma S(a^{2m} + a^{2n})$$

gleich

$$\frac{p-1}{2} \cdot (p-1) - \left[\left(\frac{p-1}{2}\right)^2 - \left(\frac{p-1}{2}\right)\right];$$

dieselbe Grösse ist dagegen gleich

$$-\left(\frac{p-1}{2}\right)^2,$$

wenn p von der Form $4i+3$ ist. Man erhält also

$$(3). \qquad y_1^2 + y_2^2 = \frac{1 + p(-1)^{\frac{p-1}{2}}}{2}.$$

Aus den Gleichungen (2) und (3) folgt

$$(4). \qquad y_1 y_2 = \frac{1 - p(-1)^{\frac{p-1}{2}}}{4},$$

und die Gleichung, welche y_1 und y_2 zu Wurzeln hat, ist somit

$$(5). \qquad y^2 + y + \frac{1 - p(-1)^{\frac{p-1}{2}}}{4} = 0,$$

oder

$$(2y+1)^2 - p(-1)^{\frac{p-1}{2}} = 0.$$

537. Wir betrachten jetzt die Gleichung, welche die $\frac{p-1}{2}$ Wurzeln der Gleichung (1), deren Summe y_1 bezeichnet, zu Wurzeln hat. Diese Gleichung sei

$$(6). \; X_1 = x^{\frac{p-1}{2}} - y_1 x^{\frac{p-1}{2}-1} + A_2 x^{\frac{p-1}{2}-2} + \cdots + A_k x^{\frac{p-1}{2}-k} + \cdots = 0.$$

Die Coefficienten $A_2, A_3, \ldots$ können durch rationale Functionen von y_1 ausgedrückt werden, und man darf (No. 182) diese Functionen als linear ansehen, da y_1 Wurzel einer Gleichung zweiten Grades ist. Der Coefficient A_k ist also von der Form

$$A_k = m_k + n_k y_1,$$

wo m_k und n_k rationale Zahlen sind, und es lässt sich leicht be-

weisen, dass m_k, n_k sogar ganze Zahlen sein müssen. A_k ist nämlich, abgesehen von seinem Vorzeichen, gleich der Summe der Producte von je k der $\frac{p-1}{2}$ Wurzeln r^{a^2}, r^{a^4}, ... Jedes dieser Produkte ist eine Potenz von r und reducirt sich folglich auf die Einheit, oder auf eine Wurzel der Gleichung (1). Man hat daher

$$A_k = \alpha_0 + \alpha_1 r + \alpha_2 r^a + \alpha_3 r^{a^2} + \cdots + \alpha_{p-1} r^{a^{p-2}},$$

wo α_0, α_1, ... ganze Zahlen sind. Dieser Werth von A_k ändert sich nicht, wenn man r in r^{a^2} verwandelt; mithin ist

$$A_k = \alpha_0 + \alpha_1 r^{a^2} + \alpha_2 r^{a^3} + \alpha_3 r^{a^4} + \alpha_4 r^{a^5} + \cdots + \alpha_{p-1} r^a.$$

Wir behaupten nun, dass in diesen beiden Werthen von A_k die Coefficienten derselben Potenzen von r einander gleich sein müssen. Nehmen wir einmal an, dies sei nicht der Fall. Setzt man die beiden Werthe von A_k einander gleich und macht die Exponenten von r mittels der Gleichung $r^p = 1$ kleiner als p, so erhält man eine Gleichung $(p-1)^{\text{ten}}$ Grades in r, welche offenbar durch $r = 1$ befriedigt wird. Diese Wurzel 1 kann man unterdrücken und sieht sodann, dass r eine Wurzel einer Gleichung $(p-2)^{\text{ten}}$ Grades mit commensurabelen Coefficienten ist. Dies ist unmöglich, da die Gleichung (1) irreductibel ist. Man hat also

$$\alpha_1 = \alpha_3 = \alpha_5 = \cdots = \alpha_{p-2},$$
$$\alpha_2 = \alpha_4 = \alpha_6 = \cdots = \alpha_{p-1},$$

folglich

$$A_k = \alpha_0 + \alpha_1 y_1 + \alpha_2 y_2.$$

Eliminirt man endlich y_2 mittels der Gleichung (2), so nimmt der Werth von A_k die Form an:

$$A_k = m_k + n_k y_1,$$

wo m_k, n_k positive oder negative ganze Zahlen bezeichnen.

Das Produkt der Wurzeln der Gleichung (6), nämlich

$$r^{a^2 + a^4 + \cdots + a^{p-1}},$$

ist gleich 1, mit Ausnahme des Falles $p = 3$; denn da a eine primitive Wurzel von p ist, so ist der Exponent

$$a^2 + a^4 + \cdots + a^{p-1} = \frac{a^2(a^{p-1}-1)}{a^2-1}$$

durch p theilbar. Man hat also

$$A_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}.$$

Wir wollen jetzt die Coefficienten A_k und $A_{k'}$ zweier von den Enden von X_1 gleich weit entfernten Terme vergleichen. Zwischen den Indices k und k' besteht die Relation $k + k' = \frac{p-1}{2}$. Die Grösse $(-1)^k A_k$ ist eine Summe von Potenzen von r, und die Summe der Umkehrungen derselben Potenzen ist gleich $(-1)^{k'} A_{k'}$, da das Produkt aller Wurzeln von (6) gleich 1 ist. Dies vorausgesetzt, bleiben die Reihen

$$r^a, r^{a^3}, \ldots, r^{a^{p-2}},$$
$$r^{a^2}, r^{a^4}, \ldots, r^{a^{p-1}}$$

im Falle $p = 4i + 1$ unverändert, wenn man r in $\frac{1}{r}$ verwandelt. In diesem Falle ist daher

$$A_{k'} = A_k = m_k + n_k y_1.$$

Wenn $p = 4i + 3$ ist, so geht jede der beiden Reihen

$$r^a, r^{a^3}, \ldots, r^{a^{p-2}},$$
$$r^{a^2}, r^{a^4}, \ldots, r^{a^{p-1}}$$

in die andere über, wenn man r in $\frac{1}{r}$ verwandelt. Ausserdem ist die eine der beiden Zahlen k, k' gerade, die andere ungerade. Die Gleichung

$$A_k = m_k + n_k y_1$$

zieht folglich

$$-A_{k'} = m_k + n_k y_2 = m_k - n_k (1 + y_1)$$

nach sich, und man hat in diesem Falle

$$A_{k'} = (n_k - m_k) + n_k y_1.$$

Daraus geht hervor, dass das Polynom X_1 auf die Form

$$X_1 = P + Q y_1$$

gebracht werden kann, worin P und Q Polynome mit ganzen Coefficienten sind, welche beziehungsweise die Grade $\frac{p-1}{2}$ und $\frac{p-3}{2}$ haben. Ausserdem ist Q ein durch x theilbares Polynom, in welchem die von den Enden gleich weit abstehenden Terme gleich und mit denselben Vorzeichen versehen sind. Das Poly-

nom P besitzt diese Eigenschaft nur in dem Falle $p = 4i + 1$, und folglich ist dasselbe mit der Function $2P - Q$ der Fall. Wenn $p = 4i + 3$ ist, so sind die Coefficienten der von den Enden gleich weit entfernten Terme der Function $2P - Q$ einander entgegengesetzt gleich. In der That sind dann die Coefficienten von $x^{\frac{p-1}{2}-k}$ und x^k in der Function $2P - Q$

$$2m_k - n_k \text{ und } n_k - 2m_k.$$

Um die Werthe der Coefficienten $A_2, A_3, \ldots$ von X_1 zu erhalten, nehmen wir an, es sei λ eine der Zahlen

$$1, 2, 3, \ldots, (p-1),$$

und h ein ganzer Exponent, für welchen

$$a^h \equiv \lambda \ (mod.\ p)$$

ist. Endlich bezeichnen wir noch mit S_λ die Summe der λ^{ten} Potenzen der Wurzeln der Gleichung $X_1 = 0$. Dann ergiebt sich

$$S_\lambda = r^{a^{h+2}} + r^{a^{h+4}} + \cdots + r^{a^{h+p-1}},$$

und daraus geht hervor, dass $S_\lambda = y_1$ ist, wenn h gerade, d. h. wenn λ quadratischer Rest von p ist. Dagegen ist $S_\lambda = y_2$ oder gleich $-1 - y_1$, wenn h ungerade, d. h. wenn λ quadratischer Nichtrest von p ist. Auf diese Weise lernen wir die Summen der gleichen Potenzen der Wurzeln von (6) kennen, und die Coefficienten $A_2, A_3, \ldots$ lassen sich darauf mittels der Formeln

$$\begin{aligned} S_1 - y_1 &= 0, \\ S_2 - y_1 S_1 + 2A_2 &= 0, \\ S_3 - y_1 S_2 + 2A_2 S_1 + 3A_3 &= 0, \\ &\cdots\cdots \end{aligned}$$

berechnen. Wir können danach A_k durch eine ganze Function von y_1 ausdrücken und diese Function durch Anwendung der Gleichung (5) linear machen.

538. Die vorstehende Entwicklung führt zu einem wichtigen Satze, den wir nicht übergehen dürfen.

Wir wenden uns wieder zu der oben erhaltenen Gleichung

$$X_1 = P + Qy_1.$$

Verwandelt man y_1 in y_2, so folgt

$$X_2 = P + Qy_2.$$

Ausserdem hat man $X = X_1 X_2$, mithin

$$X = P^2 + PQ(y_1 + y_2) + Q^2 y_1 y_2,$$

oder, der Relationen

$$y_1 + y_2 = -1, \quad y_1 y_2 = \frac{1 - p(-1)^{\frac{p-1}{2}}}{4}$$

wegen,

$$4X = (2P - Q)^2 - (-1)^{\frac{p-1}{2}} pQ^2.$$

Dies liefert mit Rücksicht auf die obigen Bemerkungen folgenden Satz:

Lehrsatz. — Wenn p eine ungerade Primzahl ist und X das Polynom

$$x^{p-1} + x^{p-2} + \cdots + x + 1$$

bezeichnet, so hat man

$$4X = Y^2 - pZ^2 \text{ für } p = 4i + 1,$$
$$4X = Y^2 + pZ^2 \text{ für } p = 4i + 3.$$

Z ist in beiden Fällen ein Polynom $\left(\frac{p-3}{2}\right)^{\text{ten}}$ Grades mit ganzen Coefficienten, in welchem die von den Enden gleich weit abstehenden Terme gleiche Coefficienten haben. Y ist ein Polynom $\left(\frac{p-1}{2}\right)^{\text{ten}}$ Grades mit ganzen Coefficienten, in welchem die Coefficienten der von den Enden gleich weit entfernten Terme gleich und mit denselben Vorzeichen, oder gleich und mit entgegengesetzten Vorzeichen versehen sind, jenachdem $p = 4i + 1$, oder $= 4i + 3$ ist.

Unsere Betrachtung lässt, wie oben schon bemerkt wurde, den Fall $p = 3$ unberührt. Zwar besitzt die Gleichung

$$4(x^2 + x + 1) = Y^2 + 3Z^2$$

die drei Lösungen

$$Y = 2x + 1, \quad Z = 1,$$
$$Y = x + 2, \quad Z = x,$$
$$Y = x - 1, \quad Z = x + 1;$$

aber die auf irgend eine dieser Lösungen bezüglichen Polynome Y und Z genügen nicht allen Bedingungen des vorhergehenden Satzes.

Das für die Function $\frac{x^p - 1}{x - 1}$ erhaltene Resultat lässt sich end-

lich noch auf die allgemeinere Function $\frac{x^p - y^p}{x - y}$ ausdehnen, welche aus der ersteren dadurch hervorgeht, dass man x in $\frac{x}{y}$ verwandelt und sodann mit y^{p-1} multiplicirt. Man kann danach offenbar folgenden Satz aussprechen:

Wenn p eine Primzahl ist, so kann man der Gleichung

$$Y^2 - (-1)^{\frac{p-1}{2}} p Z^2 = 4 \frac{x^p - y^p}{x - y}$$

durch Werthe von Y und Z genügen, welche ganze Functionen von x und y sind.

Ueber einige Eigenschaften der resolvirenden Function der Gleichung $\frac{x^p - 1}{x - 1} = 0$.

539. Es sei wieder x irgend eine Wurzel der Gleichung $\frac{x^p - 1}{x - 1} = 0$, und a eine primitive Wurzel der Primzahl p. Ferner bezeichnen wir mit α eine beliebige Wurzel der Gleichung $\frac{x^{p-1} - 1}{x - 1} = 0$ und setzen

$$F(\alpha) = x + \alpha x^a + \alpha^2 x^{a^2} + \cdots + \alpha^{p-2} x^{a^{p-2}} = \sum_{i=0}^{i=p-2} \alpha^i x^{a^i}.$$

Dann lässt sich erstens darthun, dass

$$F(\alpha)\, F(\alpha^{-1}) = \alpha^{\frac{p-1}{2}} p$$

ist. Man hat

$$F(\alpha^{-1}) = \sum_{k=0}^{k=p-2} \alpha^{-k} x^{a^k},$$

folglich

$$F(\alpha)\, F(\alpha^{-1}) = \sum_{k=0}^{k=p-2} \sum_{i=0}^{i=p-2} \alpha^{i-k} x^{a^i + a^k}.$$

Um diese Summe auszuwerthen, wollen wir die Coefficienten der verschiedenen Potenzen von α besonders hervortreten lassen und führen zu diesem Zwecke die ganze Zahl

$$i - k = l$$

ein. Dann ist der Coefficient von α^l

$$\Sigma x^{a^{k+l}+a^k},$$

wo das Zeichen Σ sich über die $p-1$ Werthe von k

$$0, 1, 2, \ldots, (p-2)$$

erstreckt. Nun kann man

$$a^{k+l} + a^k = a^k(a^l + 1)$$

schreiben. Wenn also nicht

$$a^l + 1 \equiv 0 \ (mod.\ p),$$

d. h.

$$l = \frac{p-1}{2}$$

ist, so liefert der Ausdruck $a^k(a^l+1)$ für die verschiedenen Werthe von k und abgesehen von den Vielfachen von p die Reihe der Zahlen

$$1, 2, 3, \ldots, p-1.$$

Danach ist der Coefficient von α^l

$$x + x^2 + \cdots + x^{p-1} = -1,$$

und dieser Schluss besteht für alle Werthe

$$0, 1, 2, \ldots, p-2$$

von l, mit alleiniger Ausnahme des Falles $l = \frac{p-1}{2}$. Die auszuwerthende Doppelsumme besteht daher aus dem Produkte von -1 in die Summe der verschiedenen Potenzen von α, mit Ausnahme der Potenz $\alpha^{\frac{p-1}{2}}$, und ausserdem aus der Gruppe von Termen, welche dem Werthe $l = \frac{p-1}{2}$ entsprechen. Wenn $l = \frac{p-1}{2}$ ist, so ist der Exponent von x für alle Werthe von k der Null congruent; die in Rede stehende Gruppe wird daher durch $p-1$ Terme gebildet, deren jeder gleich $\alpha^{\frac{p-1}{2}}$ ist. Die Vereinigung dieser beiden Theile der Doppelsumme liefert das Resultat

$$\alpha^{\frac{p-1}{2}}(p-1) + \alpha^{\frac{p-1}{2}} = \alpha^{\frac{p-1}{2}}p,$$

welches den vorliegenden Satz beweist.

540. Wir wollen jetzt einen zweiten Satz herleiten, welcher im Folgenden besteht: Wenn m und n zwei beliebige ganze Zahlen bedeuten, die aber nicht durch die Relation

$$m \equiv -n \ (mod.\ p)$$

verbunden sind, so ist $F(\alpha^m)\,F(\alpha^n)$ gleich dem Produkte der Function $F(\alpha^{m+n})$ in ein Polynom $\psi(\alpha)$, dessen Coefficienten ganze Zahlen sind, also

$$F(\alpha^m)\,F(\alpha^n) = F(\alpha^{m+n})\,\psi(\alpha).$$

Man hat nämlich

$$F(\alpha^m) = \Sigma\alpha^{mi}x^{a^i},$$
$$F(\alpha^n) = \Sigma\alpha^{nk}x^{a^k},$$

folglich

$$F(\alpha^m)\,F(\alpha^n) = \Sigma\Sigma\alpha^{mi+nk}x^{a^i+a^k},$$

und es liegt uns ob, nachzuweisen, dass die Doppelsumme des zweiten Gliedes die angegebene Form hat. Zu diesem Zwecke wollen wir nicht, wie im vorigen Satze erforderlich war, die Coefficienten der verschiedenen Potenzen von α, sondern die Coefficienten der Potenzen von x hervortreten lassen. Wir fassen zunächst den Term in's Auge, welcher aus allen Werthen von i und k entsteht, für welche man

$$a^i + a^k \equiv 0\ (mod.\ p),$$

d. h.

$$i - k = \frac{p-1}{2}$$

hat. Unter dieser Bedingung verschwindet die Summe

$$\Sigma\alpha^{mi+nk} = \Sigma\alpha^{m(k+\frac{p-1}{2})+nk} = \alpha^{\frac{m(p-1)}{2}}\,\Sigma\alpha^{(m+n)k};$$

denn da $m + n$ nicht $\equiv 0\ (mod.\ p)$ ist, so bringt der Ausdruck $(m + n)k$ bekanntlich die Reihe der ganzen Zahlen hervor, die kleiner als p sind.

Um jetzt den Coefficienten irgend einer Potenz von x, deren Exponent $\equiv a^l$ sei, hervortreten zu lassen, setzen wir

$$a^i + a^k \equiv a^l (mod.\ p).$$

Dieser Coefficient ist

$$\Sigma\alpha^{mi+nk},$$

und darin hat man i und k alle Werthe zu ertheilen, welche die vorhergehende Bedingung befriedigen können. Macht man

$$i = l + \mu,$$
$$k = l + \nu,$$

so wird diese Bedingung von l unabhängig und reducirt sich auf

$$a^\mu + a^\nu \equiv 1\ (mod.\ p).$$

Wir können uns denken, dass man für einen gegebenen Werth der Primzahl p das System der durch diese Relation verbundenen Zahlen μ und ν im Voraus gebildet habe. Dann folgt

$$\Sigma\alpha^{mi+nk} = \Sigma\alpha^{m(l+\mu)+n(l+\nu)} = \alpha^{(m+n)l}\,\Sigma\,\alpha^{m\mu+n\nu}.$$

Setzt man daher

$$\psi(\alpha) = \Sigma\alpha^{m\mu+n\nu},$$

so ist der Coefficient von x^{α^l}

$$\alpha^{(m+n)l}\psi(\alpha),$$

und die Doppelsumme, wie wir behauptet hatten, gleich

$$\psi(\alpha)\,\Sigma\alpha^{(m+n)l}x^{\alpha^l} = \psi(\alpha)\,F(\alpha^{m+n}).$$

541. Diese Polynome oder vielmehr diese complexen Zahlen $\psi(\alpha)$, deren Bildung wesentlich von den ganzen Zahlen μ und ν und sodann von den Zahlen m und n abhängt, führen zu herrlichen Sätzen der Arithmetik, von denen wir einige vorführen wollen.

Wir bemerken zunächst, dass die Relation

$$F(\alpha^m)\,F(\alpha^n) = F(\alpha^{m+n})\,\psi(\alpha),$$

wenn man die Zeichen von m und n ändert,

$$F(\alpha^{-m})\,F(\alpha^{-n}) = F(\alpha^{-(m+n)})\,\psi(\alpha^{-1})$$

liefert. Multiplicirt man diese beiden Formeln, so ergiebt sich, der Relation

$$F(\alpha)\,F(\alpha^{-1}) = \alpha^{\frac{p-1}{2}}\,p$$

wegen, sofort

$$\psi(\alpha)\,\psi(\alpha^{-1}) = p.$$

Ein sehr einfacher besonderer Fall wird die volle Bedeutung dieses Resultats zeigen. Es sei

$$p \equiv 1 \pmod{4}.$$

Dann wird der Gleichung

$$\alpha^{p-1} = 1$$

durch den Werth

$$\alpha = \sqrt{-1} = i$$

genügt, und $\psi(\alpha)$, als Summe ganzer Potenzen von i, ist von der Form $a + bi$, wo a und b ganze Zahlen sind. Ausserdem hat $\frac{1}{\alpha} = \frac{1}{i}$ den Werth $-i$, so dass

$$\psi(\alpha^{-1}) = a - bi$$

ist. Folglich hat jede Primzahl, die $\equiv 1 \pmod{4}$ ist, die Form

$$(a + bi)(a - bi) = a^2 + b^2.$$

Dieser Lehrsatz, den wir in den Nummern 294 und 332 nach einer ganz anderen Methode herleiteten, findet sich hier in der Weise bewiesen, dass man a und b von den ganzen Zahlen μ und ν abhängen lässt. Aus diesem ganz unerwarteten Zusammenhange hat Jacobi eine Folgerung gezogen, die wir nur anführen wollen:

Wird die Zahl a in der Gleichung $p = a^2 + b^2$ als ungerade vorausgesetzt, so kann ihr Werth bis auf das Vorzeichen dadurch bestimmt werden, dass man den kleinsten Rest des Ausdrucks

$$\frac{1}{2} \cdot \frac{2n(2n-1)(2n-2)\cdots(n+1)}{1 \cdot 2 \ldots n} \pmod{p}$$

nimmt, wo $p = 4n + 1$ angenommen wird.

Es sei ferner

$$p \equiv 1 \pmod{3}.$$

Dann wird die Gleichung

$$\alpha^{p-1} = 1$$

durch die complexe kubische Wurzel der Einheit

$$\alpha = \frac{-1 + \sqrt{-3}}{2} = \varrho$$

befriedigt, und die Zahlen $\psi(\alpha)$ und $\psi(\alpha^{-1})$, als Summen ganzer Potenzen von ϱ, werden beziehungsweise

$$a + b\varrho\ ,\ a + b\varrho^2,$$

wo a und b ganze Zahlen sind. p ist folglich von der Form

$$(a + b\varrho)(a + b\varrho^2) = a^2 - ab + b^2.$$

542. Wir wollen noch eine Folgerung für die Auflösung der binomischen Gleichung

$$x^p = 1$$

anführen. Es sei α eine primitive Wurzel der Gleichung

$$x^{p-1} = 1,$$

und es werde

$$p = 2n + 1$$

gesetzt, so dass

$$\alpha^n = -1$$

ist. Bezeichnet allgemein $\psi_i(\alpha)$ das durch die Gleichung

$$F(\alpha)F(\alpha^i) = \psi_i(\alpha)F(\alpha^{i+1})$$

definirte Polynom in α, so erhält man die Reihe der Relationen

$$F(\alpha)\,F(\alpha) \quad = \psi_1\ (\alpha)\ F(\alpha^2),$$
$$F(\alpha)\,F(\alpha^2) \quad = \psi_2\ (\alpha)\ F(\alpha^3),$$
$$\cdots\cdots\cdots\cdots\cdots,$$
$$F(\alpha)\,F(\alpha^{n-1}) = \psi_{n-1}(\alpha)\ F(\alpha^n),$$

deren Multiplication zu dem Resultat

$$F(\alpha)^n = \psi_1(\alpha)\,\psi_2(\alpha)\ldots\psi_{n-1}(\alpha)\,F(\alpha^n)$$

führt. Da nun $\alpha^n = -1$ ist, so lässt sich der Factor $F(\alpha^n)$ leicht auswerthen. Derselbe reducirt sich auf die Differenz der in No. 536 bestimmten Grössen y_2 und y_1. Man kann ihn aber auch aus der oben bewiesenen allgemeinen Relation

$$F(\alpha)\,F(\alpha^{-1}) = \alpha^{\frac{p-1}{2}}\,p$$

herleiten. Zu diesem Zwecke hat man darin $\alpha = -1$ zu nehmen, was aus dem Grunde erlaubt ist, weil so der Gleichung $\alpha^{p-1} = 1$ genügt wird. Man erhält auf diese Weise

$$F(-1)^2 = (-1)^{\frac{p-1}{2}}\,p,$$

und die $(p-1)^{\text{te}}$ Potenz der resolvirenden Function wird somit durch ein mit der Zahl p multiplicirtes Produkt complexer Factoren $\psi(\alpha)$ ausgedrückt.

Neuer Beweis des Legendre'schen Reciprocitätsgesetzes.

543. Die in diesem Kapitel dargelegte Theorie liefert, wie Jacobi gezeigt hat, einen neuen Beweis des in No. 332 hergeleiteten Legendre'schen Reciprocitätsgesetzes. Wir halten es für nützlich, diese wichtige Anwendung hier vorzuführen.

Wir betrachten die Gleichung

$$\frac{x^p-1}{x-1} = 0$$

und bezeichnen eine ihrer Wurzeln mit r. Ferner sei a eine primitive Wurzel der Primzahl p, und es werde

$$P = r - r^a + r^{a^2} - r^{a^3} + \cdots + r^{a^{p-3}} - r^{a^{p-2}}$$

gesetzt. Bezeichnet q eine von p verschiedene ungerade Primzahl, und wird das Polynom P auf die q^{te} Potenz erhoben, so enthält das Resultat die q^{ten} Potenzen der verschiedenen Terme von P und ausserdem noch andere Terme, deren Coefficienten sämmtlich durch q theilbar sind. Wird die Gesammtheit der letzteren Terme mit $q\Sigma A r^{\alpha}$ bezeichnet und

$$Q = r^q - r^{qa} + r^{qa^2} - \cdots + r^{qa^{p-3}} - r^{qa^{p-2}}$$

gesetzt, so ist

$$P^q = Q + q\Sigma A r^{\alpha}.$$

Es ist jetzt der Fall, in welchem $\left(\frac{q}{p}\right) = +1$ ist, von demjenigen zu unterscheiden, in welchem man $\left(\frac{q}{p}\right) = -1$ hat.

1⁰. Es sei $\left(\frac{q}{p}\right) = +1$, also q eine Wurzel der Congruenz

$$x^{\frac{p-1}{2}} - 1 \equiv 0 \ (mod.\ p),$$

deren Wurzeln

$$a^2,\ a^4,\ a^6,\ \ldots,\ a^{p-1}$$

sind. Man hat dann

$$q \equiv a^{2n} \ (mod.\ p),$$

wo n eine ganze Zahl ist, die nicht grösser als $\frac{p-1}{2}$ sein kann. Der Werth von Q ist folglich

$$Q = r^{a^{2n}} - r^{a^{2n+1}} + r^{a^{2n+2}} - \cdots + r^{a^{2n+p-3}} - r^{a^{2n+p-2}},$$

und wenn die Exponenten von a kleiner als $p-1$ gemacht werden, so ergiebt sich offenbar

$$Q = P.$$

2⁰. Es sei jetzt $\left(\frac{q}{p}\right) = -1$. In diesem Falle ist q eine Wurzel der Congruenz

$$x^{\frac{p-1}{2}} + 1 \equiv 0 \ (mod.\ p),$$

welche die Wurzeln

$$a,\ a^3,\ a^5,\ \ldots,\ a^{p-2}$$

hat. Es ist daher

$$q \equiv a^{2n+1} \ (mod.\ p),$$

wo n eine ganze Zahl ist. Dann folgt

$$Q = r^{a^{2n+1}} - r^{a^{2n+2}} + r^{a^{2n+3}} - \cdots + r^{a^{2n+p-2}} - r^{a^{2n+p-1}},$$

und wenn die Exponenten von a kleiner als $p-1$ gemacht werden,

$$Q = -P.$$

Man hat danach in allen Fällen

$$Q = \left(\frac{q}{p}\right) P,$$

folglich

$$P^q = \left(\frac{q}{p}\right) P + q \Sigma A r^\alpha,$$

oder

$$(1). \qquad P^{q-1} - \left(\frac{q}{p}\right) = q \frac{\Sigma A r^\alpha}{P}.$$

Macht man, dies vorausgesetzt,

$$y_1 = r + r^{a^2} + r^{a^4} + \cdots + r^{a^{p-3}}$$
$$y_2 = r^a + r^{a^3} + r^{a^5} + \cdots + r^{a^{p-2}},$$

so ergiebt sich (No. 536)

$$y_1 = -\tfrac{1}{2} \pm \tfrac{1}{2} \sqrt{(-1)^{\frac{p-1}{2}} p},$$
$$y_2 = -\tfrac{1}{2} \mp \tfrac{1}{2} \sqrt{(-1)^{\frac{p-1}{2}} p},$$

woraus

$$P = y_1 - y_2 = \pm \sqrt{(-1)^{\frac{p-1}{2}} p}$$

folgt. Wird dieser Werth von P in das erste Glied der Formel (1) eingesetzt, so reducirt sich dasselbe auf

$$p^{\frac{q-1}{2}} (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} - \left(\frac{q}{p}\right),$$

und diese Grösse ist eine ganze Zahl. Daher muss sich auch das zweite Glied $q \frac{\Sigma A r^\alpha}{P}$ auf eine ganze Zahl E reduciren, und man erhält

$$(\Sigma A r^\alpha)^2 = (-1)^{\frac{p-1}{2}} \frac{p E^2}{q^2}.$$

Daraus geht hervor, dass das Quadrat von $\Sigma A r^\alpha$ eine ganze und symmetrische Function der Wurzeln der Gleichung $\frac{x^p - 1}{x - 1} = 0$ ist. Der Werth dieses Quadrates ist folglich eine ganze Zahl, d. h. E ist ein Vielfaches Mq von q. Man hat also

$$q \frac{\Sigma A r^\alpha}{P} = E = Mq,$$

wo M eine ganze Zahl ist, und die Formel (1) geht über in

$$p^{\frac{q-1}{2}} \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} - \left(\frac{q}{p}\right) = Mq.$$

Beachtet man jetzt, dass

$$p^{\frac{q-1}{2}} = \left(\frac{p}{q}\right) + \text{Vielf. von } q$$

ist, und lässt beiderseits die Vielfachen von q weg, so folgt

$$(2). \qquad \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \left(\frac{q}{p}\right),$$

welche Formel eben der Ausdruck des Satzes von Legendre ist.

Viertes Kapitel.

Ueber eine Klasse von Gleichungen neunten Grades, die algebraisch auflösbar sind.

Determinante einer ganzen und homogenen Function dreier Veränderlichen.

544. In Crelle's Journal (Bd. XXVIII, p. 68 und Bd. XXXIV, p. 191) hat O. Hesse zwei wichtige Arbeiten über die Bestimmung der Inflexionspunkte der Curven dritten Grades veröffentlicht. In der zweiten dieser Arbeiten beweist er, dass die Inflexionspunkte einer algebraischen Curve n^{ten} Grades auf einer zweiten Curve vom Grade $3(n-2)$ liegen, dass folglich eine algebraische Curve n^{ten} Grades im Allgemeinen $3n(n-2)$ reelle oder imaginäre Inflexionspunkte hat.

In besonderen Fällen können einige dieser Inflexionspunkte in die Unendlichkeit fallen, oder durch vielfache Punkte ersetzt werden.

Für $n = 3$ liefert der erste der genannten Sätze das Resultat:

Die Inflexionspunkte einer Curve dritten Grades liegen auf einer zweiten Curve dritten Grades.

Daraus geht hervor, dass die Ermittlung der Inflexionspunkte einer Curve dritten Grades allgemein von der Auflösung einer Gleichung neunten Grades mit einer Unbekannten abhängt. Es ist nun sehr bemerkenswerth, dass diese Gleichung neunten Grades immer algebraisch aufgelöst werden kann, und dass es zur Ausführung ihrer Auflösung genügt, eine einzige Gleichung vierten und drei Gleichungen dritten Grades zu lösen. Dies ergiebt sich leicht, wie wir später darthun werden, aus dem oben ange-

gebenen Satze von Hesse und aus einem anderen zuerst von Maclaurin bewiesenen Satze, welcher im Folgenden besteht:

Die Gerade, welche zwei Inflexionspunkte einer Curve dritten Grades verbindet, trifft die Curve in einem dritten Inflexionspunkte.

Der Beweis, den Hesse in seiner zweiten Arbeit für die Auflösbarkeit der in Rede stehenden Gleichung neunten Grades giebt, setzt den Maclaurin'schen Satz gleichfalls voraus. Hesse zeigt, dass zwischen den Wurzeln gewisse Relationen bestehen und beweist allgemein, dass jede Gleichung neunten Grades, deren Wurzeln diese Eigenschaft haben, durch Wurzelgrössen gelöst werden kann. Am Ende dieses Kapitels werden wir diese Untersuchung von Hesse darlegen.

545. Es sei U irgend eine ganze und homogene Function n^{ten} Grades der beiden Veränderlichen x und y. Nimmt man $\frac{x}{y}$ zur Unbekannten, so ist $U = 0$ irgend eine Gleichung n^{ten} Grades, und diese Gleichung wird drei gleiche Wurzeln besitzen, wenn man gleichzeitig den drei Gleichungen

$$U = 0\,,\ \frac{dU}{dx} = 0\,,\ \frac{d^2 U}{dx^2} = 0$$

genügen kann. Diese Bedingungsgleichungen sind beziehungsweise von den Graden n, $n-1$, $n-2$. Statt ihrer kann man aber drei Gleichungen nehmen, deren jede den Grad $n-2$ hat. Sie lassen sich nämlich in folgender Weise schreiben*):

---

*) Dies geht unmittelbar aus dem „Satz von den homogenen Functionen" hervor. Ist $f(x, y, \ldots)$ eine homogene Function μ^{ten} Grades mehrerer Veränderlichen, und werden x, y, ... mit $1 + \alpha$ multiplicirt, so folgt aus der Definition der homogenen Functionen

$$f(x + \alpha x\ ,\ y + \alpha y\ ,\ \ldots) = (1 + \alpha)^{\mu} f(x, y, \ldots).$$

Entwickelt man beide Glieder dieser Formel in Beziehung auf α und setzt sodann die Coefficienten derselben Potenzen von α einander gleich, so erhält man

$$x\,\frac{df}{dx} + y\,\frac{df}{dy} + \cdots = \mu\, f(x, y, \ldots)\,,$$

$$x^2\,\frac{d^2 f}{dx^2} + 2\,xy\,\frac{d^2 f}{dx\,dy} + y^2\,\frac{d^2 f}{dy^2} + \cdots = \mu\,(\mu - 1)\, f(x, y, \ldots),$$

. . . .

$$\left\{\begin{aligned} U &= \frac{1}{n\,(n-1)}\left(x^2\frac{d^2U}{dx^2}+2\,xy\,\frac{d^2U}{dx\,dy}+y^2\frac{d^2U}{dy^2}\right)=0,\\ \frac{dU}{dx} &= \frac{1}{n-1}\left(x\,\frac{d^2U}{dx^2}+y\,\frac{d^2U}{dx\,dy}\right)=0,\\ \frac{d^2U}{dx^2} &= 0. \end{aligned}\right.$$

Der dritten Gleichung wegen reducirt sich die zweite auf

$$\frac{d^2U}{dx\,dy}=0,$$

und die erste wird sodann

$$\frac{d^2U}{dy^2}=0.$$

Damit also die Gleichung $U=0$ drei gleiche Wurzeln habe, müssen die drei Bedingungen

$$\frac{d^2U}{dx^2}=0,\ \frac{d^2U}{dx\,dy}=0,\ \frac{d^2U}{dy^2}=0$$

erfüllt sein, und jede dieser Bedingungsgleichungen ist vom Grade $n-2$.

Ebenso würde sich darthun lassen, dass die Gleichung $U=0$ allgemein m gleiche Wurzeln besitzt, wenn die Bedingungsgleichungen $(n-m+1)^{\text{ten}}$ Grades

$$\frac{d^{m-1}U}{dx^{m-1}}=0,\ \frac{d^{m-1}U}{dx^{m-2}dy}=0,\ldots,\ \frac{d^{m-1}U}{dx\,dy^{m-2}}=0,\ \frac{d^{m-1}U}{dy^{m-1}}=0$$

erfüllt sind.

546. Es sei jetzt u irgend eine ganze und homogene Function n^{ten} Grades der drei Veränderlichen x, y, z. Stellt man durch $\frac{x}{z}$ und $\frac{y}{z}$ die rechtwinkligen oder schiefwinkligen Coordinaten eines beweglichen Punktes dar, so ist

(1). $$u=0$$

die Gleichung irgend einer Curve n^{ten} Grades*).

Eine beliebige Gerade, deren Gleichung

(2). $$z=ax+by$$

---

*) Hesse hatte zuerst den schönen Gedanken, die rechtwinkligen Coordinaten eines Punktes in der Ebene durch $\frac{x}{z}$, $\frac{y}{z}$, diejenigen eines Punktes im Raume durch $\frac{x}{u}$, $\frac{y}{u}$, $\frac{z}{u}$ darzustellen. Man erreicht dadurch, dass alle Gleichungen, die man betrachtet, homogen werden.

ist, trifft die Curve bekanntlich in n Punkten. Setzt man den in (2) angegebenen Werth von z in die Function u ein, so wird letztere eine homogene Function U der beiden Veränderlichen x und y, und die n Wurzeln der Gleichung $U = 0$, in welcher $\frac{x}{y}$ als Unbekannte angesehen wird, sind die Verhältnisse der Coordinaten der Punkte, in welchen die Gerade die Curve trifft. Die Gleichung der Geraden enthält aber zwei Constanten a und b, welche in die Gleichung $U = 0$ eingeführt werden. Zwischen diesen Constanten kann man einen solchen Zusammenhang feststellen, dass zwei Wurzeln der Gleichung $U = 0$ einander gleich werden: In diesem Falle wird die Gerade eine Tangente der Curve. Giebt man den Constanten a und b solche Werthe, dass die Gleichung $U = 0$ drei gleiche Wurzeln besitzt, so wird die Gerade Tangente in einem Inflexionspunkte. Dieser Punkt bestimmt sich, wie wir oben gesehen haben, durch die drei Gleichungen

$$\frac{d^2 U}{dx^2} = 0\,,\quad \frac{d^2 U}{dx\,dy} = 0\,,\quad \frac{d^2 U}{dy^2} = 0\,.$$

Da aber U der Werth ist, welchen u für $z = ax + by$ annimmt, so lassen sich diese drei Gleichungen, wenn der Kürze wegen

$$\frac{d^2 u}{dx^2} = u_{1,1}\,,\quad \frac{d^2 u}{dy^2} = u_{2,2}\,,\quad \frac{d^2 u}{dz^2} = u_{3,3}\,,$$

$$\frac{d^2 u}{dy\,dz} = u_{2,3}\,,\quad \frac{d^2 u}{dx\,dz} = u_{3,1}\,,\quad \frac{d^2 u}{dx\,dy} = u_{1,2}$$

gemacht wird, in folgender Weise schreiben:

$$(3).\qquad \begin{cases} u_{1,1} + 2au_{3,1} + a^2 u_{3,3} = 0, \\ u_{1,2} + a\,u_{2,3} + b\,u_{3,1} + a\,b\,u_{3,3} = 0, \\ u_{2,2} + 2bu_{2,3} + b^2 u_{3,3} = 0. \end{cases}$$

Eliminirt man aus diesen Gleichungen a und b, so erhält man die Gleichung einer Curve, welche die vorgelegte Curve in den Inflexionspunkten trifft. Um diese Elimination auszuführen, lösen wir die zweite der Gleichungen (3) in Beziehung auf a auf. Den so erhaltenen Werth

$$a = -\frac{u_{1,2} + bu_{3,1}}{u_{2,3} + bu_{3,3}}$$

setzen wir in die erste Gleichung (3) ein. Es ergiebt sich

$$u_{1,1}\,(u_{2,3} + b\,u_{3,3})^2 - 2\,u_{3,1}\,(u_{1,2} + b\,u_{3,1})\,(u_{2,3} + b\,u_{3,3}) \\ + u_{3,3}\,(u_{1,2} + b\,u_{3,1})^2 = 0,$$

oder, wenn in Beziehung auf b geordnet wird,

$$u_{1,1}\ u_{2,3}^2 - 2\,u_{2,3}\ u_{3,1}\ u_{1,2} + u_{3,3}\ u_{1,2}^2$$
$$+ (u_{1,1}u_{3,3} - u_{3,1}^2)\ (2\,b\,u_{2,3} + b^2 u_{3,3}) = 0.$$

Wird endlich die dritte Gleichung (3) mit

$$u_{1,1}\ u_{3,3} - u_{3,1}^2$$

multiplicirt und vom Resultate die eben gebildete Gleichung subtrahirt, so gelangt man zur Endgleichung, welche durch Elimination von a und b entsteht. Wir stellen dieselbe durch

(4). $$\varDelta u = 0$$

dar, indem wir der Kürze wegen

(5). $$\varDelta u = u_{1,1}u_{2,2}u_{3,3} + 2u_{2,3}u_{3,1}u_{1,2} - u_{1,1}u_{2,3}^2 - u_{2,2}u_{3,1}^2 - u_{3,3}\,u_{1,2}^2$$

setzen.

Die Gleichung (4) ist die Gleichung der gesuchten Curve, welche die Curve der vorgelegten Gleichung $u = 0$ in den Inflexionspunkten trifft. Wie man sieht, ist (4) vom Grade $3\ (n-2)$; folglich hat eine Curve n^{ten} Grades im Allgemeinen $3n\ (n-2)$ Inflexionspunkte. Im Besonderen hat eine Curve dritten Grades neun Inflexionspunkte.

Die Function $\varDelta u$ ist gleich der Determinante

$$\begin{vmatrix} u_{1,1}\ , & u_{1,2}\ , & u_{1,3} \\ u_{2,1}\ , & u_{2,2}\ , & u_{2,3} \\ u_{3,1}\ , & u_{3,2}\ , & u_{3,3} \end{vmatrix},$$

und Hesse hat ihr den Namen „Determinante der Function u“ gegeben.

547. Wenn die Coefficienten der Function u unbestimmt sind, so besitzt die durch die Gleichung $u = 0$ dargestellte Curve keine vielfachen Punkte. Für solche Punkte hat man gleichzeitig

$$\frac{du}{dx} = 0,\ \frac{du}{dy} = 0\ ,\ u = 0,$$

und mittels der beiden ersten dieser Gleichungen reducirt sich die dritte dem Satze von den homogenen Functionen zufolge auf

$$\frac{du}{dz} = 0.$$

Der für das Vorhandensein vielfacher Punkte erforderliche Zusammenhang zwischen den Coefficienten von u ergiebt sich daher durch die Elimination von x und y aus

$$\frac{du}{dx} = 0, \frac{du}{dy} = 0, \frac{du}{dz} = 0.$$

Diese Gleichungen können auf die Form

$$xu_{1,1} + yu_{1,2} + zu_{1,3} = 0,$$
$$xu_{2,1} + yu_{2,2} + zu_{2,3} = 0,$$
$$xu_{3,1} + yu_{3,2} + zu_{3,3} = 0$$

gebracht werden, und daraus folgt offenbar

$$\Delta u = 0.$$

Ausserdem zeigt die Methode, nach welcher wir die Inflexionspunkte bestimmt haben, dass die etwa vorhandenen vielfachen Punkte der letzten Gleichung genügen; denn wenn die Gerade $z = ax + by$ in einem vielfachen Punkte Tangente der Curve wird, so besitzt die Gleichung, welche durch Elimination von z aus

$$u = 0 \text{ und } z = ax + by$$

entsteht, offenbar drei gleiche Wurzeln.

Es ist leicht zu sehen, dass eine Curve dritten Grades keinen dreifachen Punkt, und ebenso wenig drei Doppelpunkte haben kann, wofern sie sich nicht auf ein System von drei Geraden reducirt. Sie kann auch nicht zwei Doppelpunkte haben, wenn sie sich nicht auf ein System reducirt, das aus einem Kegelschnitte und einer Geraden besteht.

548. Die in No. 546 ausgeführte Rechnung ist von derjenigen nicht verschieden, die man anzustellen hätte, wenn man die Bedingung ermitteln wollte, unter welcher die Gerade (2) ein Theil des durch (1) dargestellten Ortes ist. In der That wird diese neue Aufgabe dadurch gelöst, dass man ausdrückt, das Resultat U der Substitution von $ax + by$ an die Stelle von z in u sei identisch Null. Man hat also

$$\frac{d^2U}{dx^2} = 0, \frac{d^2U}{dx\,dy} = 0, \frac{d^2U}{dy^2} = 0,$$

und da

$$n(n-1)\ U = x^2 \frac{d^2U}{dx^2} + 2\,xy \frac{d^2U}{dx\,dy} + y^2 \frac{d^2U}{dy^2}$$

ist, so liegt es auf der Hand, dass diese Bedingungen hinreichend sind. So bestehen in dem Falle, mit dem wir uns beschäftigen, der Gleichung (2) wegen die Gleichungen (3) identisch, und dasselbe ist folglich mit der Gleichung (4) der Fall. Jede

Gerade, welche dem Orte der Gleichung $u = 0$ angehört, ist daher auch ein Theil des Ortes der Gleichung $\Delta u = 0$.

Für den Fall $n = 3$ gilt der Satz: Wenn die Gleichung $u = 0$ drei Gerade darstellt, so machen eben dieselben Geraden den Ort der Gleichung $\Delta u = 0$ aus, und man hat folglich $\Delta u = ku$, wo k eine Constante ist.

Es kann vorkommen, dass die Determinante Δu identisch Null ist. Damit dies der Fall sei, ist erforderlich und hinreichend, dass die Gleichung $u = 0$ ein Büschel von n Geraden darstelle. Obwohl wir diesen von Hesse gefundenen Satz nicht anzuwenden haben werden, konnten wir doch nicht umhin, ihn zu erwähnen.

Ueber die Inflexionspunkte der Curven dritten Grades.

549. Wir wollen jetzt in Betreff der Curven dritten Grades einige allgemeine Sätze herleiten, auf die wir uns später stützen werden.

Wir erinnern zunächst daran, dass das aus einem Kegelschnitte und einer Geraden, sowie das aus drei Geraden bestehende System Varietäten der Curven dritten Grades sind.

Hilfssatz I. — Zwei Curven dritten Grades schneiden sich im Allgemeinen in neun Punkten.

Es ergiebt sich dies unmittelbar aus dem Bezout'schen Satze über den Grad der Endgleichung, welche durch Elimination einer Unbekannten aus zwei Gleichungen entsteht.

550. Hilfssatz II. — Zur Bestimmung einer Curve dritten Grades genügen im Allgemeinen neun Punkte.

Die allgemeine Gleichung der Curven dritten Grades enthält zehn Terme. Der Coefficient eines dieser Terme kann nach Belieben gewählt werden. Es sind dann noch neun Coefficienten unbestimmt, über die man so verfügen kann, dass die Curve durch neun gegebene Punkte geht. Auf diese Weise erhält man neun Gleichungen ersten Grades zwischen den unbestimmten Coefficienten. Diese Gleichungen lassen im Allgemeinen nur eine Lösung zu, und es lässt sich folglich durch neun gegebene Punkte nur eine Curve dritten Grades legen*).

---

*) In seinen schönen Untersuchungen über die Curven dritten und vierten Grades (Comptes rendus de l'Académie des Sciences, t. XXVI,

Zusatz. — Wenn $u=0$, $v=0$ die Gleichungen zweier auf rechtwinklige Coordinatenaxen bezogenen Curven dritten Grades sind, so ist

$$v + \lambda u = 0,$$

wo λ eine unbestimmte Constante bezeichnet, die allgemeine Gleichung der Curven dritten Grades, welche durch die gemeinschaftlichen Punkte der gegebenen Curven gehen.

Zunächst leuchtet ein, dass die Gleichung $v + \lambda u = 0$ eine Curve darstellt, welche durch die Schnittpunkte der gegebenen Curven hindurchgeht. Zweitens sei C irgend eine der Curven dritten Grades, welche durch diese neun Punkte gehen. Wir nehmen auf dieser Curve einen beliebigen Punkt M an, welcher den gegebenen Curven nicht angehört, und bezeichnen die Werthe, welche u und v für diesen Punkt haben, mit u_1 und v_1. Bestimmt man dann λ durch die Bedingung $v_1 + \lambda u_1 = 0$, so geht die Curve, deren Gleichung $v + \lambda u = 0$ ist, durch M. Sie hat somit zehn Punkte mit der Curve C gemeinschaftlich, d. h. sie fällt mit C zusammen.

Der vorstehende Beweis nimmt keine Rücksicht auf den Fall, in welchem die Oerter der Gleichungen $u=0$, $v=0$ eine Gerade oder einen Kegelschnitt gemeinschaftlich haben. In diesem Falle hat man aber

$$v = tv', \quad u = tu'.$$

$v'=0$, $u'=0$ stellen Gerade oder Kegelschnitte, und $v' + \lambda u' = 0$ stellt jede Gerade oder jeden Kegelschnitt dar, welcher durch die Schnittpunkte der ersteren hindurch geht. Daraus folgt, dass $v + \lambda u = 0$ auch jetzt noch alle Curven dritten Grades darstellt, welche durch die den vorgelegten Curven gemeinschaftlichen Punkte gehen.

551. Hilfssatz III. — Es seien A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8, A_9 die neun Schnittpunkte zweier gegebenen Curven dritten Grades. Durch irgend sieben dieser Punkte kann man unendlich viele Curven dritten Gra-

---

p. 943 und t. XXVII, p. 272, 437, 472) lehrt Chasles zwei Methoden, die Curve dritten Grades, welche durch neun gegebene Punkte geht, zu construiren.

des hindurch legen, welche durch keinen der beiden übrigen Punkte gehen.

Wir betrachten die sieben Punkte

$$A_1 , A_2 , A_3 , A_4 , A_5 , A_6 , A_7 .$$

Liegen drei derselben, etwa A_1, A_2, A_3, in gerader Linie, so giebt es drei aus je zwei Geraden gebildete Systeme, deren jedes die vier Punkte A_4, A_5, A_6, A_7 enthält. Eine dieser sechs Geraden kann durch A_8 oder durch A_9 gehen. Sie kann aber diese beiden Punkte nicht gleichzeitig enthalten, da nicht mehr als drei Punkte einer Curve dritten Grades in einer Geraden liegen können. Unter unseren Systemen von Geraden giebt es daher wenigstens eins, welches keinen der Punkte A_8, A_9 enthält. Dieses System bildet in Verbindung mit der Geraden $A_1\, A_2\, A_3$ eine Curve dritter Ordnung, welche die angegebene Bedingung erfüllt.

Wenn sechs der betrachteten sieben Punkte auf einem Kegelschnitte liegen, so hat derselbe mit keiner der beiden gegebenen Curven noch einen weiteren Punkt gemeinschaftlich; er geht also weder durch A_8, noch durch A_9. Verbindet man daher mit diesem Kegelschnitte eine durch den siebenten der betrachteten Punkte beliebig gezogene Gerade, welche weder durch A_8, noch durch A_9 geht, so erhält man eine Curve dritter Ordnung, welche gleichfalls der aufgestellten Bedingung genügt.

Wir nehmen jetzt an, dass von den betrachteten sieben Punkten weder sechs auf einem Kegelschnitte, noch drei in einer Geraden liegen. Verbindet man den Punkt A_7 mit den sechs übrigen Punkten, so geht höchstens eine der erhaltenen sechs Geraden

$$A_1\, A_7 , A_2\, A_7 , A_3\, A_7 , A_4\, A_7 , A_5\, A_7 , A_6\, A_7$$

durch A_8, und ebenso höchstens eine derselben durch A_9. Wir dürfen daher voraussetzen, dass

$$A_3\, A_7 , A_4\, A_7 , A_5\, A_7 , A_6\, A_7$$

weder durch A_8, noch durch A_9 gehen. Verbindet man weiter A_6 mit den Punkten A_3, A_4, A_5, so erhält man die drei Geraden

$$A_3\, A_6 , A_4\, A_6 , A_5\, A_6 ,$$

unter denen sich wenigstens eine vorfindet, die weder durch A_8, noch durch A_9 geht. Daraus folgt, dass man von den sieben betrachteten Punkten immer drei, z. B.

$$A_5 , A_6 , A_7 ,$$

wählen kann, die so beschaffen sind, dass die je zwei derselben verbindenden Geraden durch keinen der beiden Punkte A_8, A_9 gehen.

Dies vorausgesetzt, betrachten wir die Curven dritten Grades, welche beziehungsweise aus den durch

$$A_1, A_2, A_3, A_4, A_5 \; ; \; A_1, A_2, A_3, A_4, A_6 \; ; \; A_1, A_2, A_3, A_4, A_7$$

gehenden Kegelschnitten und den Geraden

$$A_6 A_7 \; , \; A_5 A_7 \; , \; A_5 A_6$$

gebildet sind. Einer der Kegelschnitte kann einen der Punkte A_8, A_9, aber nicht beide enthalten, da ein Kegelschnitt mit einer Curve dritten Grades nicht mehr als sechs Punkte gemeinschaftlich haben kann. Ferner können zwei unserer Kegelschnitte keinen Punkt ausser A_1, A_2, A_3, A_4 gemeinschaftlich haben; folglich enthält einer derselben, z. B. $A_1 A_2 A_3 A_4 A_5$ weder A_8, noch A_9. Wird mit diesem Kegelschnitte die Gerade $A_6 A_7$ verbunden, so erhält man eine Curve dritten Grades, welche der angegebenen Bedingung genügt.

Wir können somit in allen Fällen eine Curve dritten Grades ermitteln, welche durch die betrachteten sieben Punkte geht und keinen der beiden übrigen Punkte enthält. Ist

$$w = 0$$

die Gleichung dieser auf zwei Coordinatenaxen bezogenen Curve, und sind

$$u = 0 \; , \; v = 0$$

die Gleichungen der gegebenen Curven, a und b zwei willkürliche Constanten, so stellt die Gleichung

$$au + bv + w = 0$$

offenbar eine unendliche Menge von Curven dritten Grades dar, welche der angegebenen Bedingung sämmtlich genügen.

552. Lehrsatz I. — Jede Curve dritten Grades, welche durch acht Schnittpunkte zweier gegebenen Curven dritten Grades geht, geht auch durch den neunten Schnittpunkt dieser Curven.

Es seien Γ und Γ_1 die beiden gegebenen Curven dritten Grades. Nehmen wir an, man wolle eine Curve dritten Grades durch die neun Schnittpunkte der Curven Γ und Γ_1 hindurch legen. Die neun linearen Gleichungen, welche die Coefficienten der Glei-

chung der unbekannten Curve befriedigen müssen, lassen die beiden Lösungen zu, welche sich auf die der Aufgabe genügenden Curven Γ und Γ_1 beziehen. Daraus geht hervor, dass das System dieser neun Gleichungen unbestimmt ist. Ausserdem sind irgendwelche acht derselben nach dem Hilfssatze III verschieden und ziehen folglich die neunte nach sich. Daraus ziehen wir den Schluss: Wenn man eine Curve dritten Grades Γ_2 der Bedingung unterwirft, durch acht der den Curven Γ und Γ_1 gemeinschaftlichen Punkte zu gehen, und wenn man, um die Bestimmung von Γ_2 zu vollenden, eine beliebige neue Bedingung aufstellt, so muss die Curve Γ_2 durch den neunten Schnittpunkt von Γ und Γ_1 gehen.

Zusatz I. — Wenn drei Schnittpunkte zweier Curven dritten Grades auf einer Geraden liegen, so liegen die sechs übrigen Schnittpunkte auf einem Kegelschnitte.

Die Gerade, welche durch die drei ersten Schnittpunkte der gegebenen Curven Γ und Γ_1 geht, und der durch fünf von den sechs übrigen Schnittpunkten gelegte Kegelschnitt bilden nämlich eine Curve dritten Grades, welche nach dem vorhergehenden Lehrsatze auch durch den neunten Schnittpunkt von Γ und Γ_1 geht. Da es nun unmöglich ist, dass vier Punkte einer Curve dritten Grades in einer Geraden liegen, so muss dieser neunte Punkt dem Kegelschnitte angehören.

Zusatz II. — Wenn sechs Schnittpunkte zweier Curven dritten Grades auf einem Kegelschnitte liegen, so liegen die drei übrigen Schnittpunkte in einer Geraden.

Der Kegelschnitt, welcher durch die sechs ersten Schnittpunkte geht, und die Gerade, welche zwei der drei übrigen Schnittpunkte verbindet, bilden eine Curve dritten Grades, auf welcher der neunte Schnittpunkt liegen muss. Da nun ein Kegelschnitt mit einer Curve dritten Grades nicht mehr als sechs Punkte gemeinschaftlich haben kann, so muss die Gerade durch diesen neunten Punkt gehen.

Zusatz III. — Wenn drei Schnittpunkte zweier Curven dritten Grades in einer Geraden und drei der sechs übrigen Schnittpunkte gleichfalls in einer Ge-

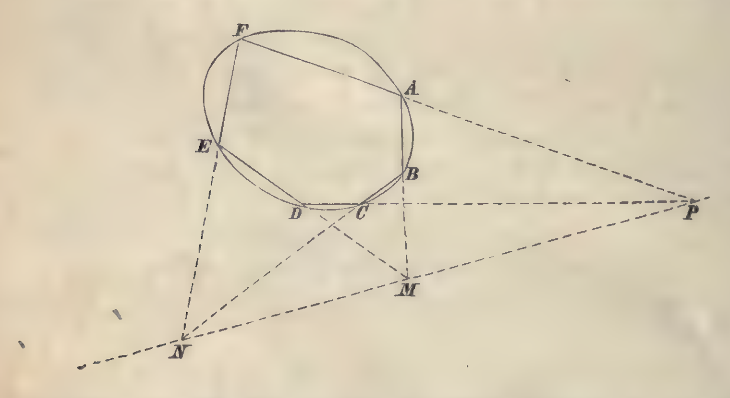
raden liegen, so liegen auch die drei letzten Schnittpunkte in einer Geraden.

Dieser Zusatz ist offenbar ein besonderer Fall des vorhergehenden.

553. Die im Vorhergehenden entwickelten Sätze führen zu vielen interessanten Folgerungen. Um uns aber nicht zu weit von unserem Gegenstande zu entfernen, wollen wir nur zeigen, wie man daraus unmittelbar den bekannten Pascal'schen Satz über das einem Kegelschnitte eingeschriebene Sechseck herleitet. Dieser Satz besteht im Folgenden:

Die Schnittpunkte der gegenüberliegenden Seiten eines einem Kegelschnitte eingeschriebenen Sechsecks liegen in einer Geraden.

Es seien A, B, C, D, E, F die Ecken des Sechsecks, M, N, P die Durchschnittspunkte der Seiten AB und DE, BC und EF, CD und FA. Die beiden Curven dritten Grades, von denen die eine aus den Geraden AB, CD, EF, die andere aus den

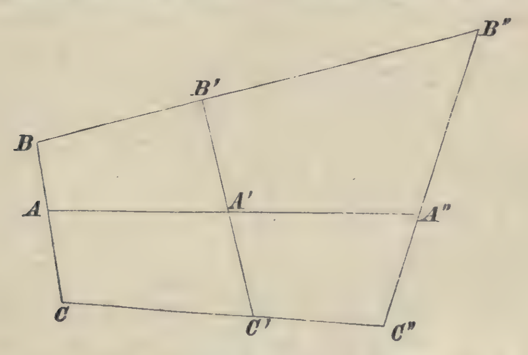


Geraden BC, DE, FA besteht, schneiden einander in den neun Punkten $A, B, C, D, E, F, M, N, P$. Da nun die sechs ersten Punkte einem Kegelschnitte angehören, so liegen die drei letzten in einer Geraden, w. z. b. w.

554. Lehrsatz II. — Die Gerade, welche zwei Inflexionspunkte einer Curve dritten Grades verbindet, trifft die Curve in einem dritten Inflexionspunkte.

Es seien A und A' zwei Inflexionspunkte einer Curve dritten Grades Γ. Wir nehmen an, die Gerade AA' treffe die Curve

Γ in dem dritten Punkte A'', und behaupten, A'' sei gleichfalls ein Inflexionspunkt. Dies zu beweisen, ziehen wir durch A eine beliebige Sekante, welche die Curve noch in den Punkten B und C treffen möge. Eine zweite beliebige Sekante ziehen wir durch A'; dieselbe möge die Curve noch in B' und C' treffen. Darauf verbinden wir B mit B', C mit C' und nehmen an, dass diese Sekanten mit der Curve beziehungsweise noch die Punkte B'' und C'' gemeinschaftlich haben. Endlich ziehen wir die Gerade



$A''B''$. Die aus den drei Geraden ABC, $A'B'C'$ und $A''B''$ bestehende Linie dritten Grades geht durch acht Durchschnittspunkte der Curve Γ mit der durch die drei Geraden $AA'A''$, $BB'B''$, $CC'C''$ gebildeten Linie dritten Grades. Sie muss daher auch durch den neunten Durchschnittspunkt C'' gehen, und da es unmöglich ist, dass vier Punkte einer Curve dritten Grades in einer Geraden liegen, so muss die Gerade $A''B''$ durch den Punkt C'' gehen. Denken wir uns jetzt die Sekanten BC und $B'C'$ beziehungsweise so um die Punkte A und A' gedreht, dass sie Tangenten der Curve werden. Da A und A' zwei Inflexionspunkte sind, so kommen im Grenzfalle B und C auf A, und ebenso B' und C' auf A' zu liegen. Die Geraden $BB'B''$ und $CC'C''$ fallen also mit $AA'A''$ zusammen, und folglich vereinigen sich die drei Durchschnittspunkte der Curve und der Sekante $A''B''C''$ in A''. Dieser Punkt A'' ist daher ein Inflexionspunkt.

Anmerkung. — Obwohl die Form dieses Beweises geometrisch ist, so lässt sich derselbe doch, wie man leicht sieht, ebenso wohl auf den Fall imaginärer, wie auf denjenigen reeller Punkte anwenden.

555. Lehrsatz III. — Die Anzahl der Geraden, deren

jede durch drei Inflexionspunkte einer gegebenen Curve dritten Grades geht, ist gleich zwölf. Diese zwölf Geraden bilden vier Systeme von je drei Geraden, und die neun Inflexionspunkte der Curve liegen zu je dreien auf den drei Geraden jedes Systems.

Verbindet man einen der Inflexionspunkte der Curve mit den acht übrigen durch gerade Linien, so müssen letztere sich augenscheinlich auf vier verschiedene Gerade reduciren; denn die Verbindungslinie zweier Inflexionspunkte geht noch durch einen dritten Inflexionspunkt, und mehr als drei Inflexionspunkte können auf einer Geraden nicht liegen. Von den Geraden, welche je drei der neun Inflexionspunkte verbinden, gehen also immer vier durch einen dieser Punkte. Rechnet man für jeden Inflexionspunkt vier Gerade, so ergeben sich 4×9 oder 36 Gerade. Dann ist aber jede Gerade offenbar dreimal gezählt. Die Anzahl derselben ist daher 12.

Betrachten wir eine der vier Geraden, welche durch ein und denselben Inflexionspunkt gehen. Diese Gerade enthält drei Inflexionspunkte, und durch jeden derselben gehen nur drei andere unserer zwölf Geraden. Folglich giebt es unter diesen zwölf Geraden zwei, welche durch keinen der drei ersten Punkte gehen. Eine derselben enthält daher drei neue Inflexionspunkte, und die drei letzten Punkte müssen dann auf der zweiten dieser beiden Geraden liegen, da die neun Punkte zweien Curven dritten Grades gemeinschaftlich sind (No. 552, Zusatz III). Wir schliessen daraus, dass die betrachteten zwölf Geraden vier Systeme von je drei Geraden bilden, welche durch die neun Inflexionspunkte gehen.

556. Um zu erkennen, nach welchem Gesetze sich die neun Inflexionspunkte auf die eben betrachteten zwölf Geraden vertheilen, kann man mit Erfolg die von Galois in die Zahlentheorie eingeführte Betrachtung der Imaginären anwenden. Wir bezeichnen die in Rede stehenden Punkte durch einen Buchstaben, der mit einem Index versehen ist, welcher neun verschiedene Werthe annehmen kann. Als die Werthe dieses Index nehmen wir die neun Wurzeln $ai + b$ der Congruenz

$$i^9 - i \equiv 0 \ (mod. \ 3).$$

Eine dieser Wurzeln ist Null, die übrigen acht sind den Potenzen einer primitiven Wurzel der Congruenz

$$i^8 - 1 \equiv 0 \ (mod.\ 3)$$

congruent. Diese Congruenz hat vier primitive Wurzeln. Es sind dies die Wurzeln der beiden irreductibelen Congruenzen

$$i^2 - i - 1 \equiv 0 \ , \ i^2 + i - 1 \equiv 0 \ (mod.\ 3).$$

Bezeichnet i eine Wurzel der ersten dieser beiden Congruenzen, so ist

$$i^2 \equiv i + 1 \ (mod.\ 3),$$

folglich

$$\left.\begin{array}{ll} i^3 \equiv 2i + 1 \ , & i^6 \equiv 2i + 2 \ , \\ i^4 \equiv 2 \ , & i^7 \equiv i + 2 \ , \\ i^5 \equiv 2i \ , & i^8 \equiv 1 \end{array}\right\} (mod.\ 3).$$

Dies vorausgesetzt, betrachten wir eins der vier Systeme von drei Geraden, welche durch die neun Inflexionspunkte gehen, und ertheilen den auf diesen Geraden liegenden Punkten beziehungsweise die Indices der drei Reihen der folgenden Tabelle:

$$(1). \qquad \left\{\begin{array}{lll} 0 \ , & 1 \ , & 2 \ , \\ i \ , & i + 1 \ , & i + 2 \ , \\ 2i \ , & 2i + 1 \ , & 2i + 2. \end{array}\right.$$

Um die Combinationen der Indices zu bilden, welche irgend einer der neun übrigen Linien entsprechen, muss man drei Indices nehmen, welche beziehungsweise den drei Reihen der Tabelle (1) angehören, und da die auf einer der Geraden des ersten Systems liegenden drei Punkte sich durch Nichts unterscheiden so kann man voraussetzen, dass jede Verticalreihe der Tabelle (1) dreien auf derselben Geraden liegenden Punkten entspricht. Man erhält also das zweite System

$$(2). \qquad \left\{\begin{array}{lll} 0 \ , & i \ , & 2i \ , \\ 1 \ , & i + 1 \ , & 2i + 1 \ , \\ 2 \ , & i + 2 \ , & 2i + 2. \end{array}\right.$$

In jedem der beiden noch zu bildenden letzten Systeme müssen die ein und derselben Geraden entsprechenden Indices drei verschiedenen Horizontalreihen jeder der Tabellen (1) und (2) angehören. Mit Rücksicht darauf ergeben sich als die einzig möglichen Combinationen:

$$(3). \qquad \left\{\begin{array}{lll} 0 \ , & i + 1 \ , & 2i + 2 \ , \\ 1 \ , & i + 2 \ , & 2i \ , \\ 2 \ , & i \ , & 2i + 1 \ , \end{array}\right.$$

und

$$(4).\qquad \begin{cases} 0\ ,\ i+2\ ,\ 2i+1, \\ 1\ ,\ i, \qquad\ \ 2i+2, \\ 2\ ,\ i+1\ ,\ 2i. \end{cases}$$

Ersetzt man jeden Ausdruck $ai + b$ durch die ihm congruente Potenz von i, so findet man, dass die auf unsere vier Systeme von Geraden bezüglichen Indices allgemein durch

$$(5).\qquad \begin{cases} 0 \quad\ \ ,\ i^m \quad\ ,\ i^{m+4}, \\ i^{m+1}\ ,\ i^{m+2}\ ,\ i^{m+7}, \\ i^{m+3}\ ,\ i^{m+5}\ ,\ i^{m+6} \end{cases}$$

dargestellt sein werden, wenn man m der Reihe nach vier beliebige aufeinanderfolgende Werthe, z. B. 0, 1, 2, 3 ertheilt.

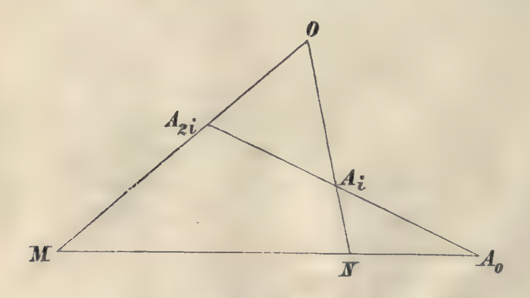
Was die neun Büschel von je vier in einem Inflexionspunkte zusammentreffenden Geraden betrifft, so werden deren Indices durch

$$(6).\qquad \begin{cases} z\ ,\ z+1, \qquad\ ,\ z+2, \\ z\ ,\ z+i, \qquad\ ,\ z+2i, \\ z\ ,\ z+i+1\ ,\ z+2i+2, \\ z\ ,\ z+i+2\ ,\ z+2i+1 \end{cases}$$

dargestellt, worin z der Reihe nach die neun Werthe der Form $ai + b$ annehmen muss.

557. Lehrsatz IV. — Von den neun Inflexionspunkten einer reellen Curve dritten Grades sind immer drei reell und sechs imaginär.

Wir beweisen zunächst, dass die neun Inflexionspunkte nicht sämmtlich reell sein können. Nehmen wir an, dies wäre der



Fall und betrachten das Dreieck OMN, welches durch die drei Geraden eines der vier Systeme gebildet wird, deren Vorhanden-

sein wir nachgewiesen haben. Gesetzt etwa, die Seiten MN, NO, OM bildeten das erste System von drei Geraden und enthielten beziehungsweise die Punkte

$$\begin{array}{lll} A_0 \;, & A_1 \;, & A_2 \;, \\ A_i \;, & A_{i+1} \;, & A_{i+2}, \\ A_{2i} \;, & A_{2i+1} \;, & A_{2i+2}. \end{array}$$

Wendet man die bekannte Eigenschaft der Transversalen auf die Schnittpunkte der von A_0 ausgehenden drei Geraden

$$A_0\, A_i\, A_{2i} \;,\; A_0\, A_{i+1}\, A_{2i+2} \;,\; A_0\, A_{i+2}\, A_{2i+1}$$

mit dem Dreieck OMN an, so ergiebt sich

$$\frac{MA_0}{NA_0} \cdot \frac{NA_i}{OA_i} \cdot \frac{OA_{2i}}{MA_{2i}} = 1,$$

$$\frac{MA_0}{NA_0} \cdot \frac{NA_{i+1}}{OA_{i+1}} \cdot \frac{OA_{2i+2}}{MA_{2i+2}} = 1,$$

$$\frac{MA_0}{NA_0} \cdot \frac{NA_{i+2}}{OA_{i+2}} \cdot \frac{OA_{2i+1}}{MA_{2i+1}} = 1,$$

und die Multiplication dieser Formeln liefert

$$\left(\frac{MA_0}{NA_0}\right)^3 = \frac{MA_{2i} \cdot MA_{2i+1} \cdot MA_{2i+2}}{OA_{2i} \cdot OA_{2i+1} \cdot OA_{2i+2}} \times \frac{OA_i \cdot OA_{i+1} \cdot OA_{i+2}}{NA_i \cdot NA_{i+1} \cdot NA_{i+2}}.$$

Es liegt auf der Hand, dass man denselben Werth für

$$\left(\frac{MA_1}{NA_1}\right)^3 \text{ und für } \left(\frac{MA_2}{NA_2}\right)^3$$

erhält, wenn man denselben Satz auf die von den Punkten A_1 und A_2 ausgehenden Geraden anwendet. Man hat daher

$$\left(\frac{MA_0}{NA_0}\right)^3 = \left(\frac{MA_1}{NA_1}\right)^3 = \left(\frac{MA_2}{NA_2}\right)^3.$$

Da die betrachteten Punkte als reell vorausgesetzt werden, so zieht diese Relation die folgende nach sich:

$$\frac{MA_0}{NA_0} = \frac{MA_1}{NA_1} = \frac{MA_2}{NA_2},$$

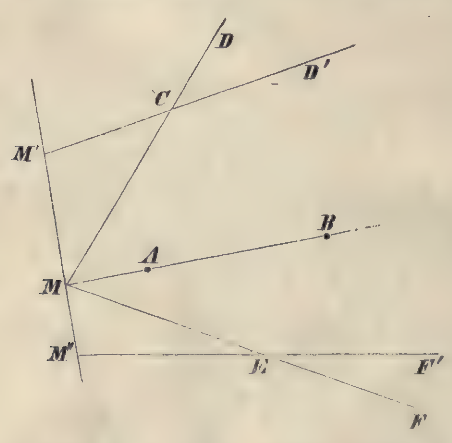
und diese ist offenbar unmöglich.

Dies vorausgesetzt, betrachten wir das Büschel, welches entsteht, wenn man einen imaginären Inflexionspunkt mit den übrigen Punkten verbindet. Irgend eine der vier Geraden dieses Büchels schneidet die Curve dritten Grades in zwei Inflexionspunkten, welche nicht beide reell und auch nicht conjugirte ima-

ginäre Punkte sein können. Eine dieser Geraden enthält den zum Scheitel des Büschels conjugirten und ausserdem einen reellen Punkt. Jede der übrigen Geraden enthält wenigstens einen neuen imaginären Punkt, und da die Anzahl der imaginären Punkte gerade ist, so muss sie wenigstens gleich 6 sein. Da endlich die durch zwei conjugirte imaginäre Punkte gehende Gerade reell ist, so erfordert jedes Paar solcher Punkte einen reellen Inflexionspunkt. Es giebt somit stets drei reelle und sechs imaginäre Inflexionspunkte.

558. Lehrsatz V. — Zieht man durch einen Punkt M einer Curve dritten Grades Γ drei Gerade, welche die Curve nochmals beziehungsweise in den Punkten A und B, C und D, E und F treffen, so liegen die sechs Punkte A, B, C, D, E, F auf einem Kegelschnitte, wenn M ein Inflexionspunkt von Γ ist. Wenn umgekehrt die Punkte A, B, C, D, E, F auf einem Kegelschnitte liegen, so ist M ein Inflexionspunkt der Curve.

Wir ziehen durch den Punkt M eine Sekante, welche die Curve Γ von Neuem in M' und M'' trifft. Darauf verbinden wir



M' mit C und M'' mit E durch gerade Linien, welche mit Γ beziehungsweise noch die Punkte D' und F' gemeinschaftlich haben. Die neun Punkte

$$M, M', M''; \; A, B, C, E; \; D', F'$$

liegen auf der Curve Γ und auf der Linie dritten Grades, welche durch die drei Geraden

$$MAB\ ,\ M'CD'\ ,\ M''EF'$$

gebildet wird. Ausserdem liegen die Punkte M, M', M'' auf einer Geraden, folglich die sechs Punkte

$$A, B, C, E, D', F'$$

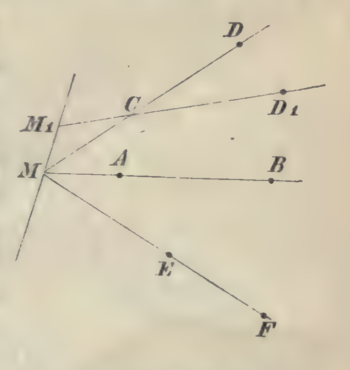
auf einem Kegelschnitte.

Dieser Schluss besteht, welches auch die Sekante $M\,M'\,M''$ ist. Lassen wir dieselbe sich um den Punkt M drehen, bis sie Tangente der Curve Γ wird, so fallen die Punkte M' und M'' zuletzt mit M zusammen, wenn M ein Inflexionspunkt ist. Dann kommen $M'CD'$ und $M''EF'$ beziehungsweise auf MCD und MEF zu liegen. Die sechs Punkte

$$A, B, C, D, E, F$$

liegen folglich auf einem Kegelschnitte.

Ist dagegen M kein Inflexionspunkt, so fällt, wenn die Gerade $MM'M''$ Tangente der Curve Γ wird, nur einer der Punkte M', M'' mit M zusammen; der andere, etwa M', nimmt eine Grenzlage M_1 an. Ebenso wird F' mit F zusammenfallen, und D' eine gewisse Lage D_1 einnehmen. Dann liegen die sechs Punkte A, B, E, F, C, D_1 auf einem Kegelschnitte, der aber den Punkt D nicht enthalten kann, da er sonst sieben Punkte mit der Curve Γ gemeinschaftlich haben würde.



Zusatz I. — Zieht man durch einen Punkt M einer Curve dritten Grades Γ Sekanten an diese Curve und nimmt das harmonische Mittel der beiden Segmente jeder Sekante, so liegen die erhaltenen Theilpunkte in gerader Linie, wenn M ein Inflexionspunkt ist. Wenn umgekehrt der geometrische Ort der harmonischen Punkte eine gerade Linie ist, so ist M ein Inflexionspunkt der Curve Γ.

Wenn nämlich M ein Inflexionspunkt ist, und man drei Sekanten MAB, MCD, MEF zieht, so liegen die Punkte A, B, C, D, E, F auf einem Kegelschnitte, und die Polare des Punktes M in Beziehung auf diesen Kegelschnitt schneidet jede

Sekante in einem Punkte, dessen Abstand von M das harmonische Mittel der beiden Segmente der Sekante ist.

Es sei jetzt M kein Inflexionspunkt. Zieht man in M die Tangente MM_1, welche die Curve vom Neuen in M_1 trifft, und verbindet M_1 mit C durch eine Gerade, welche die Curve noch in D_1 schneidet, so liegen die Punkte A, B, E, F, C, D_1 auf einem Kegelschnitte, welcher die Gerade MC in einem von D verschiedenen Punkte D' schneidet. Die Polare des Punktes M in Beziehung auf den Kegelschnitt schneidet jede Sekante MAB, MEF, MCD' in einem Punkte, dessen Entfernung von M das harmonische Mittel der Segmente der Sekante ist, und es liegt auf der Hand, dass dasselbe nicht mit den Segmenten MC, MD der Fall sein kann.

Zusatz II. — Die neun Inflexionspunkte einer gegebenen Curve dritten Grades sind auch die Inflexionspunkte aller Curven dritten Grades, die sie sämmtlich enthalten.

Es sei M ein Inflexionspunkt einer Curve dritten Grades Γ. Wir betrachten das Büschel der von M ausgehenden vier Geraden, deren jede zwei weitere Inflexionspunkte enthält. Nimmt man auf jedem Strahl das harmonische Mittel der Segmente, so liegen die vier Theilpunkte nach dem Zusatze I in einer Geraden, und daher ist M Inflexionspunkt für jede der Curven dritten Grades, die man durch die neun Inflexionspunkte der gegebenen Curve hindurch legen kann.

Zusatz III. — Wenn u eine ganze und homogene Function dritten Grades dreier Veränderlichen bezeichnet, Δ allgemein die Determinante einer solchen Function darstellt und λ irgend eine gegebene Constante ist, so hat man identisch

$$\Delta(\lambda u + \Delta u) = Au + B\Delta u,$$

wo A und B Constanten sind.

Die Gleichung $u = 0$ stellt eine Curve dar, deren Inflexionspunkte auch auf der Curve der Gleichung $\Delta u = 0$ liegen. Will man die Inflexionspunkte der Curve erhalten, welche

$$\lambda u + \Delta u = 0$$

zur Gleichung hat, so muss man ebenso mit dieser Gleichung

$$\Delta(\lambda u + \Delta u) = 0$$

verbinden. Dem Zusatze II zufolge stellt nun die letzte Gleichung eine Curve dar, welche durch die neun den Curven $u=0$, $\Delta u=0$ gemeinschaftlichen Punkte geht, deren Gleichung also von der Form

$$\mu u + \Delta u = 0 \text{ oder } Au + B\Delta u = 0$$

ist. Man hat folglich, wenn die Constanten A und B passend bestimmt werden, die Identität

$$\Delta(\lambda u + \Delta u) = Au + B\Delta u.$$

Der im Zusatze III enthaltene Satz ist von Hesse gefunden. Den Zusatz I und den Lehrsatz selbst verdanken wir Chasles. Die Folgerungen, die wir vorgeführt haben, hat zuerst Hart aus dem Lehrsatze gezogen*).

559. Lehrsatz VI. — Die rechtwinkligen Coordinaten jedes der neun Inflexionspunkte einer Curve dritten Grades lassen sich durch explicite algebraische Functionen der Coefficienten der Curven-Gleichung ausdrücken.

Es sei

$$(1). \qquad u = 0$$

die Gleichung einer Curve dritten Grades. Wie wir gesehen haben, liegen die neun Inflexionspunkte dieser Curve auch auf der Curve dritten Grades, welche

$$\Delta u = 0$$

zur Gleichung hat, so dass, wenn λ eine unbestimmte Constante bezeichnet, die Gleichung

$$(2). \qquad \lambda u + \Delta u = 0$$

allgemein alle Curven dritten Grades darstellt, welche durch die neun Inflexionspunkte der vorgelegten Curve gehen. Nun ist gezeigt worden, dass man durch diese neun Punkte vier Linien dritten Grades legen kann, deren jede aus drei Geraden besteht. Es giebt folglich vier Werthe von λ, für welche die Gleichung (2) in lineare Factoren zerfällt. Ausserdem besteht nach dem Zusatze III zum vorhergehenden Lehrsatze die Identität

$$\Delta(\lambda u + \Delta u) = Au + B\Delta u,$$

---

*) S. über diesen Gegenstand eine Note von Salmon in Crelle Journ. Bd. XXXIX, p. 365.

wo A und B offenbar ganze Functionen dritten Grades von λ sind. Die Gleichung $\lambda u + \Delta u = 0$ stellt drei Gerade dar; eben dieselben Geraden werden (No. 548) durch die Gleichung

$$\Delta(\lambda u + \Delta u) = 0 \text{ oder } Au + B\Delta u = 0$$

dargestellt. Es ist somit

(3). $$A - \lambda B = 0 \text{*)}.$$

Löst man diese Gleichung vierten Grades in λ auf, nimmt für λ irgend einen der erhaltenen Werthe und löst sodann die Gleichung (2) in Beziehung auf eine der Coordinaten, so wird man finden, dass die drei Werthe dieser Coordinate lineare Functionen der zweiten Coordinate sind. Ist die Zerlegung der Gleichung (2) in lineare Factoren auf diese Weise vollbracht, so hat man die Gleichungen von drei Geraden, deren jede drei von den neun Inflexionspunkten der vorgelegten Curve enthält, und um die Coordinaten dieser neun Punkte zu erhalten, genügt es, der Reihe nach die Lösungen zu suchen, welche der Gleichung (1) und der Gleichung jeder der drei Geraden gemeinschaftlich sind. Dies erfordert nur die Auflösung dreier Gleichungen dritten Grades mit einer Unbekannten.

Die vorstehende Betrachtung zeigt, dass die Coordinaten der neun Inflexionspunkte einer Curve dritten Grades durch explicite algebraische Functionen der Coefficienten der Curven-Gleichung ausgedrückt werden können.

Zusatz. — Die Gleichung neunten Grades, welche die Abscissen der Inflexionspunkte einer Curve dritten Grades zu Wurzeln hat, ist immer algebraisch lösbar.

Ueber einen auf die Curven dritten Grades bezüglichen Satz von Steiner.

560. Bezeichnet u eine homogene Function n^{ten} Grades der drei Veränderlichen x, y, z, so stellt die Gleichung

(1). $$u = 0$$

*) In Crelle Journ. Bd. XXXIX hat Aronhold diese Gleichung vierten Grades in λ in einer sehr bemerkenswerthen Form erhalten. Ihre Coefficienten lassen sich nämlich durch nur zwei Functionen der Coefficienten der Gleichung der vorgelegten Curve ausdrücken.

eine Curve n^{ten} Grades dar, deren Coordinaten $\frac{x}{z}$, $\frac{y}{z}$ sind.

Die Gleichung der Tangente in einem Punkte (x, y, z) der Curve (1) ist

$$\left(\frac{X}{Z} - \frac{x}{z}\right)\frac{du}{dx} + \left(\frac{Y}{Z} - \frac{y}{z}\right)\frac{du}{dy} = 0.$$

Addirt man den Term

$$\left(\frac{Z}{Z} - \frac{z}{z}\right)\frac{du}{dz},$$

welcher identisch Null ist, so nimmt diese Gleichung, der Relation

$$x\frac{du}{dx} + y\frac{du}{dy} + z\frac{du}{dz} = nu = 0$$

wegen, die Form

$$X\frac{du}{dx} + Y\frac{du}{dy} + Z\frac{du}{dz} = 0 \tag{2}$$

an.

Wenn sich die Grössen X, Y, Z auf einen gegebenen Punkt M beziehen, so stellt die Gleichung (2) eine Curve $(n-1)^{\text{ten}}$ Grades dar, welche die vorgelegte Curve in $n(n-1)$ Punkten schneidet. Daraus folgt, dass man durch den gegebenen Punkt M im Allgemeinen $n(n-1)$ Tangenten an die Curve (1) ziehen kann.

Im Falle $n = 2$ stellt die Gleichung (2) eine Gerade dar, welche die Polare des Punktes M in Beziehung auf den Kegelschnitt (1) ist. Diese Gleichung (2) ändert sich nicht, wenn man X, Y, Z durch x, y, z und umgekehrt ersetzt. Setzt man nämlich, wie in No. 546,

$$\frac{d^2u}{dx^2} = u_{1,1}, \quad \frac{d^2u}{dy^2} = u_{2,2}, \quad \frac{d^2u}{dz^2} = u_{3,3},$$

$$\frac{d^2u}{dy\,dz} = u_{2,3}, \quad \frac{d^2u}{dxdz} = u_{1,3}, \quad \frac{d^2u}{dxdy} = u_{1,2},$$

so erhält man im Falle $n = 2$

$$\frac{du}{dx} = xu_{1,1} + yu_{1,2} + zu_{1,3},$$

$$\frac{du}{dy} = xu_{2,1} + yu_{2,2} + zu_{2,3},$$

$$\frac{du}{dz} = xu_{3,1} + yu_{3,2} + zu_{3,3},$$

und da hier die Grössen $u_{1,1}$, $u_{1,2}$, ... Constanten sind, so genügt es zur Rechtfertigung unserer Behauptung, die vorstehenden Ausdrücke in die Gleichung (2) zu substituiren.

561. Betrachten wir jetzt den Fall $n = 3$. Die Gleichung (2) stellt dann einen Kegelschnitt dar, welcher auf der vorgelegten Curve die Berührungspunkte der sechs Tangenten bestimmt, die man an dieselbe durch den gegebenen Punkt ziehen kann. Wird die Gleichung (2) der Kürze wegen durch

$$v = 0$$

dargestellt, so ist der Mittelpunkt des Kegelschnitts durch die Gleichungen

$$\frac{dv}{dx} = 0 \ , \ \frac{dv}{dy} = 0$$

bestimmt.

Will man jetzt die Bedingung ermitteln, unter welcher der Kegelschnitt (2) sich auf das System von zwei Geraden reducirt, so hat man nur auszudrücken, dass die drei letzten Gleichungen durch dieselben Werthe von x und von y befriedigt werden. Nun wird $v = 0$ durch die beiden letzten Gleichungen auf $\frac{dv}{dz} = 0$ reducirt. Die gesuchte Bedingung ergiebt sich somit durch Elimination von x und y aus den drei linearen Gleichungen

$$\frac{dv}{dx} = 0 \ , \ \frac{dv}{dy} = 0 \ , \ \frac{dv}{dz} = 0.$$

Diese Gleichungen gehen aus der Gleichung (2) dadurch hervor, dass man darin u der Reihe nach durch $\frac{du}{dx}$, $\frac{du}{dy}$, $\frac{du}{dz}$ ersetzt. Sie bleiben also nach dem Früheren unverändert, wenn man X, Y, Z durch x, y, z und umgekehrt ersetzt, und man kann ihnen somit die Form

$$(3). \quad \begin{cases} x\,U_{1,1} + y\,U_{1,2} + z\,U_{1,3} = 0, \\ x\,U_{2,1} + y\,U_{2,2} + z\,U_{2,3} = 0, \\ x\,U_{3,1} + y\,U_{3,2} + z\,U_{3,3} = 0 \end{cases}$$

geben, wo die Zeichen U, $U_{1,1}$, $U_{1,2}$, ... das darstellen, was aus u, $u_{1,1}$, $u_{1,2}$, ... wird, wenn man X, Y, Z statt x, y, z schreibt.

Die Elimination von x und y aus den Gleichungen (3) liefert

$$(4). \quad \Delta U = 0,$$

wo ΔU die Determinante von U ist, und man erhält auf diese Weise den folgenden Satz:

Lehrsatz I. — Es seien u eine ganze und homogene Function dritten Grades der Veränderlichen x, y, z, und Δu die Determinante von u. Ferner seien U und ΔU das, was aus u und Δu wird, wenn man X, Y, Z statt x, y, z schreibt. Damit die Berührungspunkte der vom Punkte (X, Y, Z) an die Curve $u = 0$ gezogenen sechs Tangenten auf zwei Geraden liegen, ist erforderlich und hinreichend, dass man

$$\Delta U = 0$$

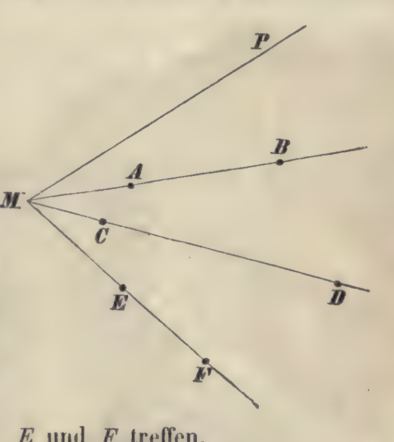
habe.

Aus diesem Satze ziehen wir die wichtige Folgerung:

Zusatz. — Durch einen Inflexionspunkt einer Curve dritten Grades kann man, abgesehen von der Tangente, welche die Curve im Inflexionspunkte berührt, drei Tangenten an diese Curve ziehen, und die Berührungspunkte der Curve mit diesen drei Tangenten liegen auf einer Geraden.

562. Die vorhergehenden Betrachtungen setzen uns in den Stand, den nachstehenden Satz zu beweisen, welchen Steiner ohne Beweis im Journal de Mathématiques pures et appliquées, t. XI veröffentlicht hat.

Lehrsatz II. — Eine Curve dritten Grades enthält im Allgemeinen 27 Punkte, in deren jedem sie eine Berührung fünfter Ordnung mit einem Kegelschnitte haben kann. Die Gleichung 27ten Grades, welche diese 27 Punkte bestimmt, ist immer algebraisch auflösbar.



Es sei P ein Punkt der gegebenen Curve. Wir ziehen in P eine Tangente an die Curve, welche die Curve von Neuem in M trifft. Durch den Punkt M ziehen wir endlich drei Secanten, welche die Curve beziehungsweise noch in den Punkten A und B, C und D, E und F treffen.

Wenn M ein Inflexionspunkt ist, so liegen die sechs Punkte A, B, C, D, E, F auf einem Kegelschnitte (No. 558). Lässt man die Sekanten so variiren, dass sie sämmtlich sich der Lage MP nähern, so variirt auch der Kegelschnitt, und im Grenzfalle hat derselbe mit der gegebenen Curve sechs zusammenfallende Punkte gemeinschaftlich, d. h. in P findet eine Berührung fünfter Ordnung statt.

Ist aber M kein Inflexionspunkt, so geht der durch die Punkte B, C, D, E, F bestimmte Kegelschnitt nicht durch den Punkt A, so nahe auch MAB an MP liegen mag, und schneidet die gegebene Curve in einem sechsten Punkte A'. Im Grenzfalle wird also der Kegelschnitt zwar wie im ersten Falle die gegebene Curve in P berühren; er schneidet dieselbe aber in einem neuen Punkte und hat mit ihr nur eine Berührung vierter Ordnung.

Daraus geht hervor, dass nur die Berührungspunkte P der durch die Inflexionspunkte an die gegebene Curve gelegten Tangenten die im Satze angegebene Eigenschaft besitzen, und da man durch jeden Inflexionspunkt drei Tangenten ziehen kann, so ist die Gesammtzahl der Punkte P gleich 3×9 oder 27.

Endlich lassen sich die Coordinaten der Inflexionspunkte durch explicite algebraische Functionen der Coefficienten der Gleichung ausdrücken, welche die gegebene Curve darstellt. Ausserdem hängt die Bestimmung der drei Punkte P, welche ein und demselben Punkte M entsprechen, nur von der Auflösung einer Gleichung dritten Grades ab. Folglich ist die Gleichung 27ten Grades, welche die 27 Punkte P bestimmt, stets algebraisch lösbar.

Eigenschaft der Gleichung neunten Grades, welche die Abscissen der Inflexionspunkte einer Curve dritten Grades zu Wurzeln hat.

563. Es sei

$$u = 0 \tag{1}$$

die Gleichung einer Curve dritten Grades zwischen den rechtwinkligen Coordinaten $\frac{x}{z}$ und $\frac{y}{z}$. Wir haben gesehen, dass die Inflexionspunkte dieser Curve auf einer zweiten Curve dritten Grades liegen, deren Gleichung

(2). $$\varDelta u = 0$$

ist. Eliminirt man aus (1) und (2) y, so erhält man eine in Beziehung auf x und z homogene Gleichung neunten Grades

(3). $$v = 0.$$

Wie oben gezeigt wurde, ist diese Gleichung, deren Wurzeln $\frac{x}{z}$ die Abscissen der Inflexionspunkte darstellen, stets algebraisch auflösbar. Zwischen den Wurzeln der Gleichung (3) bestehen nun bemerkenswerthe Relationen, aus denen Hesse die algebraische Auflösbarkeit dieser Gleichung hergeleitet hat. Diese Relationen wollen wir jetzt nach Hesse kennen lernen.

Vorher machen wir noch darauf aufmerksam, dass der jeder Wurzel $\frac{x}{z}$ von (3) entsprechende Werth von $\frac{y}{z}$ sich rational durch $\frac{x}{z}$ und die bekannten Grössen der Gleichung (1) ausdrücken lässt. Dies ergiebt sich unmittelbar aus der in No. 73 mitgetheilten Methode zur Auflösung zweier simultanen Gleichungen. Danach müssen die Coordinaten jedes Inflexionspunktes der vorgelegten Curve ein und derselben Gleichung von der Form

(4). $$\frac{y}{z} = F\left(\frac{x}{z}\right)$$

genügen, wo F eine rationale Function bezeichnet.

Es seien jetzt

$$\frac{x_0}{z_0}, \frac{y_0}{z_0} \text{ und } \frac{x_1}{z_1}, \frac{y_1}{z_1}$$

die Coordinaten zweier Inflexionspunkte der Curve (1). Die Gerade, welche durch diese Punkte hindurchgeht, hat die Gleichung

$$\frac{\frac{x}{z} - \frac{x_0}{z_0}}{\frac{x}{z} - \frac{x_1}{z_1}} = \frac{\frac{y}{z} - \frac{y_0}{z_0}}{\frac{y}{z} - \frac{y_1}{z_1}}.$$

Wird der Werth jedes Gliedes dieser Gleichung mit $-\lambda\frac{z_1}{z_0}$ bezeichnet, so folgt

$$\frac{x}{z}(z_0 + \lambda z_1) = x_0 + \lambda x_1,$$

$$\frac{y}{z}(z_0 + \lambda z_1) = y_0 + \lambda y_1.$$

Man kann über z so verfügen, dass $z = z_0 + \lambda z_1$ ist; dann lässt sich unsere Gerade, wie man sieht, durch die drei Gleichungen

$$(5). \qquad x = x_0 + \lambda x_1\,, \; y = y_0 + \lambda y_1\,, \; z = z_0 + \lambda z_1$$

darstellen, mittels welcher man alle Punkte der Geraden erhält, wenn man λ alle möglichen Werthe ertheilt. Nun schneidet diese Gerade, dem in No. 554 bewiesenen Maclaurin'schen Satze zufolge, die Curve (1) in einem dritten Inflexionspunkte. Um den Werth von λ zu ermitteln, welcher diesem dritten Punkte zukommt, hat man die in (5) angegebenen Werthe von x, y, z in die Gleichung (1) zu substituiren, und die so erhaltene Gleichung nach λ aufzulösen. Durch diese Substitution ergiebt sich

$$(6). \quad \begin{cases} (u)_0 + \lambda \left[x_1 \left(\frac{du}{dx}\right)_0 + y_1 \left(\frac{du}{dy}\right)_0 + z_1 \left(\frac{du}{dz}\right)_0\right] \\ \qquad + \lambda^2 \left[x_0 \left(\frac{du}{dx}\right)_1 + y_0 \left(\frac{du}{dy}\right)_1 + z_0 \left(\frac{du}{dz}\right)_1\right] + \lambda^3 (u)_1 = 0, \end{cases}$$

wo die Indices 0 und 1 anzeigen, dass man in den damit behafteten Ausdrücken x_0, y_0, z_0 oder x_1, y_1, z_1 satt x, y, z schreiben soll. In der That folgt aus der Taylor'schen Formel unmittelbar, dass die beiden ersten Terme von u nach der Substitution folgende sind:

$$(u)_0 + \lambda \left[x_1 \left(\frac{du}{dx}\right)_0 + y_1 \left(\frac{du}{dy}\right)_0 + z_1 \left(\frac{du}{dz}\right)_0\right],$$

und aus diesen müssen die beiden letzten Terme offenbar dadurch hervorgehen, dass man x_0, y_0, z_0, x_1, y_1, z_1 in

$$\lambda x_1\,, \lambda y_1\,, \lambda z_1\,, \frac{1}{\lambda} x_0\,, \frac{1}{\lambda} y_0\,, \frac{1}{\lambda} z_0$$

verwandelt. Die Terme $(u)_0$ und $(u)_1$ sind gleich Null und können folglich unterdrückt werden. Wird sodann die Gleichung (6) durch λ dividirt, so liefert sie folgenden Werth von λ:

$$(7). \qquad \lambda = - \frac{x_1 \left(\frac{du}{dx}\right)_0 + y_1 \left(\frac{du}{dy}\right)_0 + z_1 \left(\frac{du}{dz}\right)_0}{x_0 \left(\frac{du}{dx}\right)_1 + y_0 \left(\frac{du}{dy}\right)_1 + z_0 \left(\frac{du}{dz}\right)_1},$$

welcher dem dritten Inflexionspunkte entspricht. Bezeichnet man die Coordinaten dieses Punktes mit $\frac{x_2}{z_2}$, $\frac{y_2}{z_2}$ und setzt den eben gefundenen Werth von λ in die Gleichungen (5) ein, so erhält man

$$\frac{x_2}{z_2} = \frac{x_0\left[x_0\left(\frac{du}{dx}\right)_1 + y_0\left(\frac{du}{dy}\right)_1 + z_0\left(\frac{du}{dz}\right)_1\right] - x_1\left[x_1\left(\frac{du}{dx}\right)_0 + y_1\left(\frac{du}{dy}\right)_0 + z_1\left(\frac{du}{dz}\right)_0\right]}{z_0\left[x_0\left(\frac{du}{dx}\right)_1 + y_0\left(\frac{du}{dy}\right)_1 + z_0\left(\frac{du}{dz}\right)_1\right] - z_1\left[x_1\left(\frac{du}{dx}\right)_0 + y_1\left(\frac{du}{dy}\right)_0 + z_1\left(\frac{du}{dz}\right)_0\right]},$$

$$\frac{y_2}{z_2} = \frac{y_0\left[x_0\left(\frac{du}{dx}\right)_1 + y_0\left(\frac{du}{dy}\right)_1 + z_0\left(\frac{du}{dz}\right)_1\right] - y_1\left[x_1\left(\frac{du}{dx}\right)_0 + y_1\left(\frac{du}{dy}\right)_0 + z_1\left(\frac{du}{dz}\right)_0\right]}{z_0\left[x_0\left(\frac{du}{dx}\right)_1 + y_0\left(\frac{du}{dy}\right)_1 + z_0\left(\frac{du}{dz}\right)_1\right] - z_1\left[x_1\left(\frac{du}{dx}\right)_0 + y_1\left(\frac{du}{dy}\right)_0 + z_1\left(\frac{du}{dz}\right)_0\right]}.$$

Betrachten wir im Besonderen die erste dieser Gleichungen. Das zweite Glied derselben bleibt unverändert, wenn man x_0, y_0, z_0 in x_1, y_1, z_1 und umgekehrt verwandelt. Werden Zähler und Nenner dieses Gliedes durch $z_0{}^2 z_1{}^2$ dividirt, so nimmt es die Form

$$f\left(\frac{x_0}{z_0}, \frac{y_0}{z_0}, \frac{x_1}{z_1}, \frac{y_1}{z_1}\right)$$

an, wo f eine rationale Function bezeichnet, welche durch die Transposition der Indices 0 und 1 keine Aenderung erleidet. Nun ist nach Gleichung (4)

$$\frac{y_0}{z_0} = F\left(\frac{x_0}{z_0}\right), \quad \frac{y_1}{z_1} = F\left(\frac{x_1}{z_1}\right),$$

wo F eine rationale Function bezeichnet. Folglich kann der Werth von $\frac{x_2}{z_2}$ auf die Form

$$\frac{x_2}{z_2} = \Theta\left(\frac{x_0}{z_0}, \frac{x_1}{z_1}\right)$$

reducirt werden; darin bezeichnet Θ eine Function, welche in Beziehung auf die beiden in ihr enthaltenen Grössen rational und symmetrisch ist. Es liegt auf der Hand, dass die letzte Gleichung bestehen bleibt, wenn man die Indices 0, 1, 2 einer Substitution unterwirft. Denn man würde zu den Gleichungen, welche diese Substitutionen liefern, direkt gelangt sein, wenn man vom ersten und dritten, oder vom zweiten und dritten, statt vom ersten und zweiten Inflexionspunkte ausgegangen wäre. Die Abscissen $\frac{x_0}{z_0}$, $\frac{x_1}{z_1}$, $\frac{x_2}{z_2}$ von drei in einer Geraden liegenden Inflexionspunkten genügen somit den drei Relationen

$$\frac{x_0}{z_0} = \Theta\left(\frac{x_1}{z_1}, \frac{x_2}{z_2}\right), \quad \frac{x_1}{z_1} = \Theta\left(\frac{x_2}{z_2}, \frac{x_0}{z_0}\right), \quad \frac{x_2}{z_2} = \Theta\left(\frac{x_0}{z_0}, \frac{x_1}{z_1}\right),$$

wo Θ eine rationale und symmetrische Function bezeichnet. Auf dieser Eigenschaft beruht, wie wir sehen werden, die Auflösbarkeit der Gleichung (3).

Ueber die algebraische Auflösung einer Klasse von Gleichungen neunten Grades.

564. Es war von Interesse, die specielle Frage, mit der wir uns im Vorhergehenden beschäftigt haben, mit einer allgemeineren Theorie in Verbindung zu setzen. Das vollbrachte Hesse durch Herleitung des folgenden Satzes:

Lehrsatz. — Es seien

(1). $$\chi(x) = 0$$

eine Gleichung neunten Grades und Θ eine gegebene rationale und symmetrische Function zweier Veränderlichen. Wenn irgend zwei Wurzeln x_λ und x_μ der vorgelegten Gleichung eine dritte Wurzel $x_\varkappa$ in der Weise liefern, dass man zu gleicher Zeit

(2). $$x_\varkappa = \Theta(x_\lambda, x_\mu) \ , \ x_\lambda = \Theta(x_\mu, x_\varkappa) \ , \ x_\mu = \Theta(x_\varkappa, x_\lambda)$$

hat, so ist die Gleichung algebraisch lösbar.

Man sieht, dass der Gleichung, welche die Abscissen der Inflexionspunkte einer Curve dritten Grades zu Wurzeln hat, die in Rede stehende Eigenschaft zukommt.

Drei Wurzeln der Gleichung (1), welche den Relationen (2) genügen, nennt Hesse conjugirte Wurzeln. Es ist klar, dass jede Wurzel vier Combinationen von je drei conjugirten Wurzeln angehört. Man würde folglich, wenn man für jede Wurzel vier Combinationen rechnete, 4×9 oder 36 Combinationen erhalten. Da aber jede derselben dreimal gerechnet ist, so giebt es nur zwölf verschiedene Combinationen conjugirter Wurzeln. Die Gesammtzahl der Combinationen von je drei Wurzeln ist $\frac{9 \cdot 8 \cdot 7}{1 \cdot 2 \cdot 3}$ oder 84; es sind somit 72 Combinationen von je drei nicht conjugirten Wurzeln möglich.

Wir betrachten irgend eine der vier Gruppen conjugirter Wurzeln und bezeichnen dieselbe mit

$$x_\varkappa x_\lambda x_\mu \ , \ x_{\varkappa'} x_{\lambda'} x_{\mu'} \ , \ x_{\varkappa''} x_{\lambda''} x_{\mu''} .$$

Man darf voraussetzen, die Wurzeln $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$ seien nicht conjugirt; man kann dieselben folglich als beliebige nicht conjugirte Wurzeln ansehen. Dann erhält man, da Nichts die Indices λ und μ, λ' und μ', λ'' und μ'' von einander unterscheidet, die folgenden drei Combinationen conjugirter Wurzeln:

$$x_{\varkappa'} x_{\varkappa''} x_\lambda \;,\; x_{\varkappa''} x_\varkappa x_{\lambda'} \;,\; x_\varkappa x_{\varkappa'} x_{\lambda''} \,,$$

so dass die sechs übrigen Combinationen conjugirter Wurzeln folgende sein müssen:

$$x_\varkappa x_{\mu'} x_{\mu''} \;,\; x_{\varkappa'} x_{\mu''} x_\mu \;,\; x_{\varkappa''} x_\mu x_{\mu'};$$
$$x_{\lambda'} x_{\lambda''} x_\mu \;,\; x_{\lambda''} x_\lambda x_{\mu'} \;,\; x_\lambda x_{\lambda'} x_{\mu''}.$$

Man sieht, dass die neuen Wurzeln rational durch drei beliebige nicht conjugirte Wurzeln $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$ ausgedrückt werden können. In der That ist

$$(3).\quad \begin{cases} x_\varkappa = x_\varkappa \,,\; x_\lambda = \Theta(x_{\varkappa'}, x_{\varkappa''}) \,,\; x_\mu = \Theta\left[\Theta(x_{\varkappa''}, x_\varkappa) \,,\, \Theta(x_\varkappa \,,\, x_{\varkappa'})\right], \\ x_{\varkappa'} = x_{\varkappa'} \,,\; x_{\lambda'} = \Theta(x_{\varkappa''}, x_\varkappa) \,,\; x_{\mu'} = \Theta\left[\Theta(x_\varkappa \,,\, x_{\varkappa'}) \,,\, \Theta(x_{\varkappa'} \,,\, x_{\varkappa''})\right], \\ x_{\varkappa''} = x_{\varkappa''} \,,\; x_{\lambda''} = \Theta(x_\varkappa \,,\, x_{\varkappa'}) \,,\; x_{\mu''} = \Theta\left[\Theta(x_{\varkappa'}, x_{\varkappa''}), \Theta(x_{\varkappa''}, x_\varkappa)\right]. \end{cases}$$

Dies vorausgesetzt, bezeichnen wir mit α eine unbestimmte Constante und bilden die symmetrische Function von irgendwelchen drei conjugirten Wurzeln $x_\varkappa$, x_λ, x_μ

$$(4).\qquad y_{\varkappa,\lambda,\mu} = (\alpha - x_\varkappa)(\alpha - x_\lambda)(\alpha - x_\mu),$$

welche in Beziehung auf α vom dritten Grade ist. Werden $x_\varkappa$, x_λ, x_μ durch die Wurzeln jeder der zwölf Combinationen conjugirter Wurzeln ersetzt, so erhält man die zwölf verschiedenen Werthe der Function $y_{\varkappa,\lambda,\mu}$.

Sodann bilden wir die symmetrische Function

$$(5).\qquad z = (\beta - y_{\varkappa,\lambda,\mu})(\beta - y_{\varkappa',\lambda',\mu'})(\beta - y_{\varkappa'',\lambda'',\mu''}),$$

welche in Beziehung auf die unbestimmte Grösse β vom dritten Grade ist. Es seien z_0, z_1, z_2, z_3 die vier Werthe, welche z annimmt, wenn man darin für $y_{\varkappa,\lambda,\mu}$, $y_{\varkappa',\lambda',\mu'}$, $y_{\varkappa'',\lambda'',\mu''}$ der Reihe nach die vier Gruppen von Werthen setzt, welche diesen Grössen zukommen. Endlich bilden wir noch die Gleichung vierten Grades

$$(6).\qquad z^4 + A_1 z^3 + A_2 z^2 + A_3 z + A_4 = 0,$$

welche z_0, z_1, z_2, z_3 zu Wurzeln hat.

Es lässt sich jetzt nachweisen, dass die Coefficienten der Gleichung (6) rational durch die bekannten Grössen der Gleichung (1) und der Function Θ ausgedrückt werden können. Man hat nämlich

$$(7). \quad \begin{cases} y_{\varkappa,\lambda,\mu} = (\alpha - x_\varkappa)(\alpha - x_\lambda)(\alpha - x_\mu), \\ y_{\varkappa',\lambda',\mu'} = (\alpha - x_{\varkappa'})(\alpha - x_{\lambda'})(\alpha - x_{\mu'}), \\ y_{\varkappa'',\lambda'',\mu''} = (\alpha - x_{\varkappa''})(\alpha - x_{\lambda''})(\alpha - x_{\mu''}). \end{cases}$$

Setzt man diese Werthe in die Formel (5) ein, so erhält man bei Benutzung der Formeln (3) den Werth von z, ausgedrückt als rationale Function von drei nicht conjugirten Wurzeln $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$, nämlich

$$(8). \quad z = \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''}),$$

und diese Function ψ ist in Beziehung auf $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$ symmetrisch; denn aus den Formeln (3) ist zu ersehen, dass die Vertauschung dieser drei Wurzeln die Grössen

$$y_{\varkappa,\lambda,\mu}, \; y_{\varkappa',\lambda',\mu'}, \; y_{\varkappa'',\lambda'',\mu''}$$

nur in einander überführt, wodurch der Werth von z keine Aenderung erleidet.

Wir erheben das zweite Glied der Gleichung (8) auf die m^{te} Potenz, wo m eine beliebige ganze Zahl bezeichnet, und stellen durch

$$\Sigma'' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$$

die Summe der Terme dar, welche aus $\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$ dadurch entstehen, dass man für $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$ der Reihe nach die 72 Combinationen von je drei nicht conjugirten Wurzeln nimmt. Ferner bezeichne

$$\Sigma' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$$

die Summe der Terme, welche aus $\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$ hervorgehen, wenn für $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$ der Reihe nach die zwölf Combinationen conjugirter Wurzeln genommen werden. Endlich sei

$$\Sigma \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$$

die Summe aller Terme, welche entstehen, wenn man in

$$\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$$

für $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$ alle 84 Combinationen von je drei Wurzeln nimmt. Dann ist

$$(9). \quad \begin{cases} \Sigma'' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m + \Sigma' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m \\ \qquad = \Sigma \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m. \end{cases}$$

Das zweite Glied dieser Formel (9) ist eine rationale und sym-

metrische Function aller Wurzeln und lässt sich folglich rational durch die bekannten Grössen ausdrücken. Dasselbe ist mit $\Sigma'\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$ der Fall. Da nämlich $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$ conjugirte Wurzeln sind, so hat man

$$\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m = \psi[x_\varkappa, x_{\varkappa'}, \Theta(x_\varkappa, x_{\varkappa'})]^m$$
$$= \psi[x_{\varkappa'}, x_{\varkappa''}, \Theta(x_{\varkappa'}, x_{\varkappa''})]^m = \psi[x_{\varkappa''}, x_\varkappa, \Theta(x_{\varkappa''}, x_\varkappa)]^m.$$

Daraus folgt, dass

$$\Sigma'\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$$

ein Drittel der Summe aller 36 Werthe ist, welche

$$\psi[x_\varkappa, x_{\varkappa'}, \Theta(x_\varkappa, x_{\varkappa'})]^m$$

annimmt, wenn man für $x_\varkappa$, $x_{\varkappa'}$ die 36 Combinationen von je zwei Wurzeln setzt. Wird diese Summe durch das Zeichen Σ ausgedrückt, so hat man

$$(10). \quad \Sigma'\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m = \tfrac{1}{3}\Sigma\psi[x_\varkappa, x_{\varkappa'}, \Theta(x_\varkappa, x_{\varkappa'})]^m,$$

folglich

$$(11). \quad \begin{cases} \Sigma''\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m = \Sigma\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m \\ \qquad - \tfrac{1}{3}\Sigma\psi[x_\varkappa, x_{\varkappa'}, \Theta(x_\varkappa, x_{\varkappa'})]^m, \end{cases}$$

woraus hervorgeht, dass $\Sigma''\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$ eine rationale und symmetrische Function aller Wurzeln ist, also rational durch die bekannten Grössen ausgedrückt werden kann. Beachtet man jetzt, dass den 72 Combinationen nicht conjugirter Wurzeln nur vier verschiedene Werthe der Function z^m, nämlich z_0^m, z_1^m, z_2^m, z_3^m entsprechen, und dass jeder dieser Werthe sich 18mal vorfindet, so sieht man, dass

$$(12). \quad z_0^m + z_1^m + z_2^m + z_3^m = \frac{1}{18}\Sigma''\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$$

ist. Ertheilt man der Zahl m die Werthe 1, 2, 3, 4, so liefert die Formel (12) die Potenzsummen der Wurzeln der Gleichung (6), welche zur Berechnung der Coefficienten A_1, A_2, A_3, A_4 erforderlich sind. Diese Coefficienten werden auf diese Weise rational durch die bekannten Grössen ausgedrückt.

Die Wurzeln der Gleichung (1) erhält man jetzt auf folgende Weise: Man ermittle eine beliebige Wurzel der Gleichung (6). Diese Wurzel ist nach dem Vorhergehenden eine ganze Function dritten Grades der unbestimmten Grösse β. Wird diese Function

gleich Null gesetzt, so erhält man eine Gleichung dritten Grades in β, deren Wurzeln die drei Grössen sind, welche eine der vier Gruppen bilden, in welche sich die zwölf Grössen $y_{\varkappa,\lambda,\mu}$ vertheilen. Setzt man eine dieser neuen Wurzeln gleich Null, so entsteht eine Gleichung dritten Grades in Beziehung auf die unbestimmte Grösse α. Die drei Wurzeln α dieser Gleichung sind drei conjugirte Wurzeln der Gleichung (1). Um alle Wurzeln von (1) zu erhalten, hat man in derselben Weise mit jeder der Wurzeln der Gleichung (6) zu verfahren.

Fünftes Kapitel.

Ueber die algebraisch auflösbaren Gleichungen.

Untersuchungen von Galois. Allgemeine Lehrsätze.

565. Die in den beiden vorhergehenden Kapiteln angestellten Entwicklungen haben uns zur algebraischen Auflösung gewisser Klassen von Gleichungen geführt. Sind aber diese so bemerkenswerthen Gleichungen die einzigen, welche sich algebraisch lösen lassen? Mit andern Worten, welche Gleichungen sind einer algebraischen Auflösung fähig? Dies ist die Frage, die sich uns naturgemäss aufdrängt, und welche Abel und Galois zuerst in Angriff genommen haben.

Ich werde im Folgenden die in der Arbeit von Galois: Sur les conditions de résolubilité des équations par radicaux enthaltene Theorie darlegen. Diese Arbeit wurde zum ersten Male 1846, fünfzehn Jahre nach dem Tode des Verfassers, im Journal de Mathématiques pures et appliquées, t. XI, veröffentlicht. Die von Galois gewählte Reihenfolge der Sätze ist von mir innegehalten worden; doch habe ich die Beweise meist vervollständigen müssen.

Wir haben in No. 100 und No. 515 streng definirt, welche Bedeutung die Benennungen: rationale Grösse, rationaler Divisor einer ganzen Function, irreductibele Function, irreductibele Gleichung in jedem Falle besitzen. Wir haben auch gesagt, dass eine gegebene irreductibele Gleichung reductibel werden kann, wenn man unter die bekannten Grössen gewisse Grössen aufnimmt, welche vorher nicht als bekannt angesehen wurden.

Wenn wir allgemein dahin übereinkommen, eine gewisse Irrationale, z. B. eine Wurzel einer rationalen Function der bekannten Grössen, als bekannt anzusehen, so sagen wir mit Ga-

lois: Wir adjungiren diese Function der vorgelegten Gleichung. Eine Grösse ist dann rational, wenn sie durch eine rationale Function der ursprünglich bekannten und der adjungirten Grössen ausgedrückt werden kann. So ist die Gleichung

$$x^4 + x^3 - 4x^2 - 4x + 1 = 0,$$

von welcher die Theilung des Kreises in 15 gleiche Theile abhängt, so lange irreductibel, als man nur die rationalen Zahlen als bekannt ansieht. Sie wird dagegen reductibel, wenn man ihr eine Wurzel der Gleichung

$$z^2 - 5 = 0,$$

d. h. die Wurzelgrösse $\sqrt{5}$ adjungirt. In der That ist ihr erstes Glied das Produkt der beiden Factoren

$$x^2 + \frac{1+\sqrt{5}}{2}\,x - \left(\frac{-1+\sqrt{5}}{2}\right)^2,$$

$$x^2 - \frac{-1+\sqrt{5}}{2}\,x - \left(\frac{1+\sqrt{5}}{2}\right)^2,$$

welche rationale Functionen der bekannten Grössen sind, wenn $\sqrt{5}$ unter die Zahl der letzteren aufgenommen ist.

Die Untersuchungen von Galois stützen sich auf die in No. 490 und No. 492 bewiesenen Sätze, welche auf diese Weise eine grosse Bedeutung erlangen, und auf die Eigenschaften der Systeme conjugirter Substitutionen. Galois wendet die Betrachtung der Permutationsgruppen an, von denen in No. 430 und 431 die Rede war. Wir haben es aber vorgezogen, uns an die Substitutionen zu halten. Es ist dies übrigens nur eine Formänderung der Aussprüche der Sätze, da die Permutationen nur vom Gesichtspunkte der Substitutionen aus zu betrachten sind, durch welche der Uebergang von den einen zu den anderen bewirkt wird.

566. Lehrsatz I. — Ist

$$(1). \qquad f(x) = 0$$

eine Gleichung n^{ten} Grades, deren n Wurzeln

$$(2). \qquad x_0, x_1, x_2, \ldots, x_{n-1}$$

sind, so giebt es immer ein System conjugirter Substitutionen G, welches die Doppeleigenschaft besitzt:

1⁰ dass jede rationale Function der Wurzeln, deren numerischer Werth durch die Substitutionen von G

keine Aenderung erleidet, rational durch die bekannten Grössen ausgedrückt werden kann;

2^0 dass umgekehrt jede rationale Function der Wurzeln, welche sich rational durch die bekannten Grössen ausdrücken lässt, denselben numerischen Werth behält, wenn man alle Substitutionen von G auf sie anwendet.

Es ist zu beachten, dass man hier zu den bekannten Grössen auch diejenigen zählt, welche man der Gleichung hat adjungiren können.

Es sei V eine rationale Function der Wurzeln (2) von der Beschaffenheit, dass die

$$N = 1 \,.\, 2 \ldots n$$

Functionen, welche man durch die Substitutionen aus V herleitet, ungleiche numerische Werthe haben. Man kann z. B.

$$V = \alpha_0 x_0 + \alpha_1 x_1 + \cdots + \alpha_{n-1} x_{n-1}$$

machen, wo $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ passend gewählte ganze Zahlen sind. Ferner seien

$$\mathfrak{F}(V) = 0$$

die Gleichung N^{ten} Grades, welche die N Werthe von V zu Wurzeln hat, und $F(V)$ ein irreductibeler Divisor ν^{ten} Grades des Polynoms $\mathfrak{F}(V)$. Endlich wollen wir die ν Wurzeln der Gleichung

$$(3). \qquad F(V) = 0$$

mit

$$(4). \qquad V_0, V_1, V_2, \ldots, V_{\nu-1}$$

bezeichnen.

Nach dem Lehrsatze der No. 492 können die n Wurzeln x der Gleichung (1) durch irgend eine Horizontalreihe der Tabelle

$$(5). \quad \left\{ \begin{array}{lllll} \psi_0(V_0), & \psi_1(V_0), & \psi_2(V_0), & \ldots, & \psi_{n-1}(V_0), \\ \psi_0(V_1), & \psi_1(V_1), & \psi_2(V_1), & \ldots, & \psi_{n-1}(V_1), \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot \\ \psi_0(V_{\nu-1}), & \psi_1(V_{\nu-1}), & \psi_2(V_{\nu-1}), & \ldots, & \psi_{n-1}(V_{\nu-1}) \end{array} \right.$$

dargestellt werden, wo $\psi_0(V), \psi_1(V), \ldots$ rational aus V und den bekannten Grössen zusammengesetzt sind. Die Tabelle (5) enthält also ν Permutationen der Wurzeln x, und wir haben in No. 492 bewiesen, dass diese Permutationen eine Gruppe bilden, d. h. dass die Substitutionen

$$(6).\qquad 1\,,\, S_1\,,\, S_2\,,\, \ldots\,,\, S_{\nu-1}\,,$$

durch welche man die ν Permutationen (5) aus der ersten derselben erhält, ein conjugirtes System G ausmachen. Wir behaupten nun, dieses System G besitze die im Satze angegebene Doppeleigenschaft.

Bezeichnet nämlich Ω eine rationale Function der Wurzeln (2), und wird

$$\Omega = \Phi[\psi_0(V_0)\,,\, \psi_1(V_0)\,,\, \ldots\,,\, \psi_{n-1}(V_0)]$$

gesetzt, so ist Ω eine rationale Function von V_0, und man kann

$$(7).\qquad \Omega = \Psi(V_0)$$

schreiben, wo Ψ eine rationale Function ist.

Dies vorausgesetzt, nehmen wir zunächst an, der numerische Werth von Ω werde durch die Substitutionen (6) des Systems G nicht verändert. Da diese Substitutionen dadurch ausgeführt werden können, dass man V_0 der Reihe nach durch jeden der Werthe (4) ersetzt, so erhält man

$$\Omega = \Psi(V_0) = \Psi(V_1) = \cdots = \Psi(V_{\nu-1})\,,$$

folglich

$$\Omega = \frac{1}{\nu}[\Psi(V_0) + \Psi(V_1) + \cdots + \Psi(V_{\nu-1})].$$

Das zweite Glied dieser Formel ist eine symmetrische Function der Wurzeln der Gleichung (3); folglich lässt sich Ω rational durch die bekannten Grössen ausdrücken.

Um die Umkehrung des Satzes zu beweisen, nehmen wir an, Ω sei rational durch die bekannten Grössen ausdrückbar. Dann ist nach Formel (7) V_0 eine der Wurzeln der Gleichung

$$\Psi(V) - \Omega = 0.$$

Da aber V_0 eine Wurzel der als irreductibel vorausgesetzten Gleichung (3) ist, so müssen alle Wurzeln von (3) der vorhergehenden Gleichung genügen, und man hat somit

$$\Omega = \Psi(V_0) = \Psi(V_1) = \cdots = \Psi(V_{\nu-1}).$$

Der numerische Werth von Ω erleidet also durch die Substitutionen von G keine Aenderung, und unser Satz ist vollständig bewiesen.

Der Kürze wegen werden wir die Function V die *resolvirende Function* und die irreductibele Gleichung (3) die *resolvirende Gleichung* nennen.

567. Lehrsatz II. — Jede Substitution, welche die im vorhergehenden Lehrsatze angegebene Doppeleigenschaft besitzt, gehört dem conjugirten Systeme an, dessen Existenz dieser Lehrsatz ausspricht.

Wir behalten alle in der vorigen Nummer gebrauchten Bezeichnungen bei und bezeichnen mit X eine Function der n Wurzeln $x_0, x_1, \ldots, x_{n-1}$, welche durch die Substitutionen die $N = 1 . 2 . 3 \ldots n$ numerisch verschiedenen Werthe

$$X_0, X_1, X_2, \ldots, X_{N-1}$$

annimmt. Ferner seien

$$X_0, X_1, X_2, \ldots, X_{\nu-1}$$

die ν Werthe, welche X in Folge der ν Substitutionen von G annimmt, und es werde

$$\Omega = (X - X_0)(X - X_1) \ldots (X - X_{\nu-1})$$

gesetzt, wo X eine unbestimmte Grösse bezeichnet. Der Werth der Function Ω erleidet durch die Substitutionen von G keine Aenderung. Ω lässt sich also, dem Lehrsatze I zufolge, rational durch die bekannten Grössen ausdrücken. Ausserdem ist es klar, dass der Werth von Ω sich ändert, wenn man diese Function einer im Systeme G nicht enthaltenen Substitution T unterwirft. Die Substitution T hat folglich nicht die Eigenschaften der Substitutionen von G, welche den Gegenstand des Lehrsatzes I bilden.

Die Substitutionen von G besitzen danach rücksichtlich der vorgelegten Gleichung eine Eigenschaft, die ihnen ausschliesslich zukommt. Wir wollen dieses System das der Gleichung eigene conjugirte System nennen*).

568. Lehrsatz III. — Es sei G das conjugirte System, welches einer gegebenen Gleichung n^{ten} Grades

$$(1). \qquad f(x) = 0$$

eigen ist, der mehrere Irrationale adjungirt sein können. Adjungirt man dieser Gleichung eine Wurzel z_0 einer irreductibelen Hilfsgleichung m^{ten} Grades

---

*) Galois benutzt eine dem hier in Rede stehenden conjugirten Systeme entsprechende Permutationsgruppe und nennt sie die Gruppe der Gleichung.

(2). $$\varphi(z) = 0,$$

deren Coefficienten in rationaler Form bekannt sind, und enthält, nachdem dies geschehen ist, das der Gleichung (1) eigene conjugirte System Γ nur einen Theil der Substitutionen von G, in welchem Falle die Ordnung von G ein Vielfaches der Ordnung von Γ ist, so vertheilen sich die $m = pq$ Wurzeln der Gleichung (2) in eine gewisse Anzahl p Gruppen, deren jede aus q Wurzeln besteht, nämlich:

$$\begin{array}{l} z_0\ ,\ z_0^{(1)}\ ,\ z_0^{(2)}\ ,\ \ldots,\ z_0^{(q-1)}, \\ z_1\ ,\ z_1^{(1)}\ ,\ z_1^{(2)}\ ,\ \ldots,\ z_1^{(q-1)}, \\ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot \\ z_{p-1},\ z_{p-1}^{(1)},\ z_{p-1}^{(2)},\ \ldots,\ z_{p-1}^{(q-1)}. \end{array}$$

Diese Gruppen besitzen die Eigenschaft, dass, wenn man der vorgelegten Gleichung irgend eine der Wurzeln ein und derselben Gruppe

$$z_i,\ z_i^{(1)},\ z_i^{(2)},\ \ldots,\ z_i^{(q-1)}$$

adjungirt, das der vorgelegten Gleichung eigene conjugirte System Γ_i dasselbe ist, welche Wurzel man auch adjungirt haben mag. Ausserdem sind die p conjugirten Systeme

$$\Gamma,\ \Gamma_1,\ \Gamma_2,\ \ldots,\ \Gamma_{p-1},$$

welche der Gleichung eigen werden, wenn man ihr beziehungsweise eine Wurzel jeder Gruppe adjungirt, ähnlich, so dass jedes dieser Systeme aus dem ersten dadurch hergeleitet werden kann, dass man ein und dieselbe Substitution in den Cyclen der verschiedenen Substitutionen des letzteren ausführt. Es liegt auf der Hand, dass jede Gruppe sich auf eine einzige Wurzel reducirt, wenn m eine Primzahl ist.

Wir bezeichnen wieder mit V die resolvirende Function und mit

(3). $$F(V) = 0$$

die irreductibele Gleichung ν^{ten} Grades, welche wir die resolvirende Gleichung genannt haben. Ferner seien

$$V_0\,,\ V_1\,,\ V_2\,,\ \ldots\,,\ V_{\nu-1}$$

die ν Wurzeln der Gleichung (3).

Wenn die Gleichung (3) irreductibel bleibt, nachdem man der Gleichung (1) eine Wurzel z_0 von (2) adjungirt hat, so bleibt offenbar G das der Gleichung (1) eigene conjugirte System. Anders verhält es sich dagegen, wenn die Gleichung (3) reductibel wird, und diesen Fall haben wir zu untersuchen.

Es seien $\lambda(V, z_0)$ einer der irreductibelen Factoren von $F(V)$, und μ der Grad dieses Factors. Man darf voraussetzen, dass die höchste Potenz von V im Polynome λ den Coefficienten Eins hat, und dass die übrigen Coefficienten ganze Functionen der Wurzel z_0 sind. Führen wir jetzt die Division der Polynome $F(V)$, $\lambda(V, z)$ aus, wobei z als unbestimmte Grösse angesehen wird, und bezeichnen den Quotienten und den Rest dieser Division beziehungsweise mit $\varDelta(V, z)$, $\Theta(V, z)$, so ist

$$F(V) = \lambda(V, z)\varDelta(V, z) + \Theta(V, z),$$

und nach unserer Voraussetzung hat man identisch

$$\Theta(V, z_0) = 0;$$

denn das Polynom $\Theta(V, z)$ ist höchstens vom Grade $\mu - 1$ in V, und die letzte Gleichung wird durch jede der μ Wurzeln V von

$$\lambda(V, z_0) = 0$$

befriedigt. Im Polynome $\Theta(V, z)$ müssen also die Coefficienten der verschiedenen Potenzen von V für $z = z_0$ verschwinden. Da nun die Gleichung (2) als irreductibel vorausgesetzt wird, so verschwinden diese Coefficienten auch, wenn z durch irgend eine der Wurzeln von (2) ersetzt wird.

Stellen danach

$$z_0\,,\ z_1\,,\ z_2\,,\ \ldots\,,\ z_{m-1}$$

die m Wurzeln der Gleichung (2) dar, so ist das Polynom $F(V)$ durch jede der Functionen

$$\lambda(V, z_0)\,,\ \lambda(V, z_1)\,,\ \ldots\,,\ \lambda(V, z_{m-1})$$

theilbar. Das Produkt dieser Functionen, das wir durch $\Pi(V)$ darstellen, ist eine ganze Function von V, deren Coefficienten symmetrische Functionen der Wurzeln z sind. Dasselbe kann daher rational durch die bekannten Grössen ausgedrückt werden.

Die Wurzeln der Gleichung

$$\Pi(V) = 0$$

gehören sämmtlich der Gleichung (3) an, und da diese gegenwärtig irreductibel ist, so ist das Polynom $\Pi(V)$ durch $F(V)$ theilbar. Es sei q der Exponent der höchsten in $\Pi(V)$ aufgehenden Potenz von $F(V)$, und es werde

$$\Pi(V) = [F(V)]^q \Pi_1(V)$$

gesetzt. Offenbar muss $\Pi_1(V)$ sich auf eine Constante, oder, wenn man will, auf die Einheit reduciren, da der höchste Term in unseren Polynomen den Coefficienten 1 hat. Wäre nämlich das Gegentheil der Fall, so würde $\Pi_1(V)$ durch $F(V)$ theilbar sein müssen, weil die Gleichung

$$\Pi_1(V) = 0$$

nur solche Wurzeln hat, welche der Gleichung (3) angehören. Der Exponent q würde also nicht der ihm auferlegten Bedingung genügen. Man hat also

$$\Pi(V) = [F(V)]^q$$

oder

$$(4). \qquad [F(V)]^q = \lambda(V, z_0) \,.\, \lambda(V, z_1) \ldots \lambda(V, z_{m-1}).$$

Unserer Voraussetzung nach ist das Polynom $\lambda(V, z_0)$ irreductibel, d. h. es lässt keinen Divisor zu, dessen Grad kleiner als der seinige ist, und dessen Coefficienten rationale Functionen der bekannten Grössen und der adjungirten Wurzel z_0 sind. Wir behaupten nun, dass auch das Polynom $\lambda(V, z_i)$ die Eigenschaft besitzt, keinen Divisor zuzulassen, in welchem die Coefficienten der Potenzen von V rationale Functionen der bekannten Grössen und der Wurzel z_i sind. Dies zu beweisen, nehmen wir an, es gäbe einen solchen Divisor, und stellen denselben durch $\zeta(V, z_i)$ dar. Dividiren wir $\lambda(V, z)$ durch $\zeta(V, z)$, bis wir zu einem Reste gelangen, der in Beziehung auf V von einem niedrigeren Grade als $\zeta(V, z)$ ist, so folgt, wenn $Q(V, z)$ und $R(V, z)$ den Quotienten und den Rest dieser Division bezeichnen,

$$\lambda(V, z) = \zeta(V, z) \,.\, Q(V, z) + R(V, z).$$

$R(V, z)$ ist gleich Null für $z = z_i$. Durch ein bereits oben angewandtes Schlussverfahren ergiebt sich daraus, dass derselbe Rest Null ist, welche von den Wurzeln der Gleichung (2) man auch für z substituirt. Im Besonderen erhält man

$$R(V, z_0) = 0,$$

was ausdrückt, dass $\lambda(V, z_0)$ den Divisor $\zeta(V, z_0)$ zulässt. Da

dies Ergebniss mit unserer Voraussetzung im Widerspruch steht, so ist unsere Behauptung bewiesen.

Man kann alle Wurzeln der Gleichung (3) rational durch irgend eine derselben ausdrücken. Nachdem wir uns dies in's Gedächtniss zurückgerufen haben, betrachten wir die beiden Gleichungen

$$(5). \qquad \lambda(V, z_i) = 0 \ , \ \lambda(V, z_j) = 0,$$

und bezeichnen zwei Wurzeln der ersteren mit V_α und $\vartheta(V_\alpha)$, wo ϑ eine rationale Function ist. Wir behaupten nun, dass wenn V_β eine Wurzel der zweiten Gleichung (5) ist, auch $\vartheta(V_\beta)$ diese Gleichung befriedigt. Man hat nämlich

$$\lambda(V_\alpha, z_i) = 0 \ , \ \lambda[\vartheta(V_\alpha), z_i] = 0,$$

d. h. der Gleichung

$$\lambda[\vartheta(V), z_i] = 0$$

wird genügt, wenn man V durch die Wurzel V_α der Gleichung

$$\lambda[V, z_i] = 0$$

ersetzt; sie muss daher alle Wurzeln der letzten Gleichung zulassen, da deren erstes Glied, wie wir soeben bewiesen haben, keinen Divisor besitzt, dessen Coefficienten rationale Functionen von z_i sind. Nimmt man, und dies ist gestattet, $\vartheta(V)$ als ganze Function an, so kann man sagen, das Polynom $\lambda[\vartheta(V), z_i]$ sei durch $\lambda(V, z_i)$ theilbar, oder der Rest der Division von $\lambda[\vartheta(V), z]$ durch $\lambda(V, z)$ sei für $z = z_i$ identisch gleich Null. Dann lehrt das in diesem Beweise bereits zweimal angewandte Schlussverfahren, dass derselbe Rest auch für $z = z_j$ Null, d. h. dass $\lambda[\vartheta(V), z_j]$ durch $\lambda(V, z_j)$ theilbar ist. Folglich zieht die Gleichung

$$\lambda(V_\beta, z_j) = 0$$

die folgende nach sich:

$$\lambda[\vartheta(V_\beta), z_j] = 0,$$

und diese drückt aus, dass $\vartheta(V_\beta)$ Wurzel der zweiten Gleichung (5) ist. Wir schliessen daraus, dass, wenn die Gleichungen (5) eine Wurzel gemeinschaftlich haben, alle ihre Wurzeln gemeinschaftliche sind.

Diese Betrachtung zeigt, dass im zweiten Gliede der Formel (4) sich jeder der ungleichen Factoren q mal wiederholt vorfindet.

Wendet man zur Darstellung der m Wurzeln z zwei Indices an, so erhält man

$$\begin{array}{l} \lambda(V, z_0) = \lambda(V, z_0^{(1)}) = \lambda(V, z_0^{(2)}) = \cdots = \lambda(V, z_0^{(q-1)}), \\ \lambda(V, z_1) = \lambda(V, z_1^{(1)}) = \lambda(V, z_1^{(2)}) = \cdots = \lambda(V, z_1^{(q-1)}), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \lambda(V, z_{p-1}) = \lambda(V, z_{p-1}^{(1)}) = \lambda(V, z_{p-1}^{(2)}) = \cdots = \lambda(V, z_{p-1}^{(q-1)}), \end{array}$$

und durch Ausziehung der q^{ten} Wurzel aus beiden Gliedern der Formel (4) ergiebt sich

$$(6). \qquad F(V) = \lambda(V, z_0) . \lambda(V, z_1) \ldots \lambda(V, z_{p-1}),$$

denn man darf voraussetzen, die Coefficienten der ersten Terme der Polynome F und λ seien auf die Einheit reducirt.

Fassen wir die Ergebnisse unserer bisherigen Betrachtung zusammen, so ergiebt sich Folgendes: Die m Wurzeln z vertheilen sich in p Gruppen von je q Wurzeln. Welche von den Wurzeln ein und derselben Gruppe man ausserdem der vorgelegten Gleichung adjungirt, man erzielt immer denselben Erfolg, nämlich: an die Stelle der ursprünglichen resolvirenden Gleichung denselben Divisor dieser Gleichung zu setzen. Das der vorgelegten Gleichung eigene conjugirte System wird folglich auf ein neues System reducirt, dessen Ordnung ein Divisor der Ordnung des ursprünglichen ist.

Wir haben jetzt noch die verschiedenen conjugirten Systeme $\Gamma, \Gamma_1, \ldots, \Gamma_{p-1}$ zu vergleichen, welche der vorgelegten Gleichung eigen werden, wenn man ihr beziehungsweise eine Wurzel der oben unterschiedenen Gruppen adjungirt.

Da die Wurzeln der Gleichung

$$\lambda(V, z_0) = 0$$

rationale Functionen einer dieser Wurzeln sind, so wollen wir sie durch

$$V_0, \vartheta_1(V_0), \vartheta_2(V_0), \ldots, \vartheta_{\mu-1}(V_0)$$

darstellen. Ist ferner $V_0^{(i)}$ eine Wurzel der Gleichung

$$\lambda(V, z_i) = 0,$$

so sind die Grössen

$$V_0^{(i)}, \vartheta_1(V_0^{(i)}), \vartheta_2(V_0^{(i)}), \ldots, \vartheta_{\mu-1}(V_0^{(i)}),$$

wie wir oben bemerkt haben, Wurzeln derselben Gleichung. Wir

fügen hinzu, dass dieselben verschieden sind, so dass keine Wurzel ausgelassen ist. Hätte man nämlich

$$\vartheta_\alpha(V_0^{(i)}) = \vartheta_\beta(V_0^{(i)}),$$

so würde sich, da V_0 und $V_0^{(i)}$ Wurzeln der gegenwärtig irreductibelen Gleichung (3) sind, im Widerspruch mit unserer Voraussetzung

$$\vartheta_\alpha(V_0) = \vartheta_\beta(V_0)$$

ergeben.

Wir bezeichnen jetzt mit V irgend eine Wurzel der Resolvente (3), stellen durch das Symbol

$$[V]$$

die Permutation

$$\psi_0(V), \psi_1(V), \psi_2(V), \ldots, \psi_{n-1}(V)$$

der Wurzeln der vorgelegten Gleichung dar und setzen

$$(7). \qquad [\vartheta_k(V_0)] = S_k[V_0], \; [\vartheta_k(V_0^{(i)})] = S_k^{(i)}[(V_0^{(i)})].$$

Die Substitutionen des Systems Γ sind dann

$$1, S_1, S_2, \ldots, S_{\mu-1},$$

diejenigen des Systems Γ_i

$$1, S_1^{(i)}, S_2^{(i)}, \ldots, S_{\mu-1}^{(i)}.$$

Stellt endlich T_i die Substitution dar, durch welche man von der Permutation $[V_0]$ zur Permutation $[V_0^{(i)}]$ übergeht, so ist nicht nur

$$(8). \qquad [V_0^{(i)}] = T_i[V_0],$$

sondern auch für jeden Werth von k

$$[\vartheta_k(V_0^{(i)})] = T_i[\vartheta_k(V_0)],$$

oder der ersten der Formeln (7) wegen

$$(9). \qquad [\vartheta_k(V_0^{(i)})] = T_i S_k[V_0].$$

Endlich reducirt die Formel (8) die zweite Formel (7) auf

$$(10). \qquad [\vartheta_k(V_0^{(i)})] = S_k^{(i)} T_i[V_0],$$

und der Vergleich der Formeln (9) und (10) liefert

$$(11). \qquad S_k^{(i)} T_i = T_i S_k,$$

woraus

$$(12). \qquad S_k^{(i)} = T_i S_k T_i^{-1}$$

folgt. Die Formeln (8) und (9) drücken aus, dass das conjugirte System G durch

$$(13).\quad \begin{cases} 1 \quad, S_1 \quad, S_2 \quad, \ldots, \quad S_{\mu-1}, \\ T_1 \quad, T_1 S_1 \quad, T_1 S_2 \quad, \ldots, \quad T_1 S_{\mu-1}, \\ T_2 \quad, T_2 S_1 \quad, T_2 S_2 \quad, \ldots, \quad T_2 S_{\mu-1}, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad , \\ T_{p-1}, T_{p-1} S_1, T_{p-1} S_2, \ldots, T_{p-1} S_{\mu-1} \end{cases}$$

dargestellt wird, und die Systeme $\Gamma, \Gamma_1, \ldots, \Gamma_{p-1}$ sind nach Formel (12) folgende:

$$(14).\quad \begin{cases} \Gamma \quad = 1, S_1 \quad, S_2 \quad, \ldots, S_{\mu-1}, \\ \Gamma_1 \quad = 1, T_1 S_1 T_1^{-1} \quad, T_1 S_2 T_1^{-1} \quad, \ldots, T_1 S_{\mu-1} T_1^{-1}, \\ \Gamma_2 \quad = 1, T_2 S_1 T_2^{-1} \quad, T_2 S_2 T_2^{-1} \quad, \ldots, T_2 S_{\mu-1} T_2^{-1}, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad , \\ \Gamma_{p-1} = 1, T_{p-1} S_1 T_{p-1}^{-1}, T_{p-1} S_2 T_{p-1}^{-1}, \ldots, T_{p-1} S_{\mu-1} T_{p-1}^{-1}. \end{cases}$$

Wie man sieht, sind diese Systeme ähnlich, so dass jedes derselben aus dem ersten Γ dadurch hergeleitet werden kann, dass man in den Cyclen jeder Substitution von Γ ein und dieselbe Substitution T vollzieht. Es ist somit auch der letzte Punkt unseres Satzes bewiesen.

569. Lehrsatz IV. — Wenn das der Gleichung $f(x) = 0$ eigene System G sich auf ein System niedrigerer Ordnung Γ reducirt, dadurch dass man eine Wurzel der irreductibelen Hilfsgleichung $\varphi(z) = 0$ adjungirt, und wenn man ausserdem die Wurzeln dieser Hilfsgleichung durch rationale Functionen einer derselben und der bekannten Grössen ausdrücken kann, so erleidet das System Γ keine Aenderung, wenn in den Cyclen aller seiner Substitutionen irgend eine Substitution des Systems G ausgeführt wird.

Es seien

$$z_0 \text{ und } z_i = \vartheta z_0$$

zwei Wurzeln der Hilfsgleichung; ϑ bezeichnet hier eine rationale Function. Da die Gleichung $\varphi(z) = 0$ als irreductibel vorausgesetzt wird, so lässt sie alle Wurzeln

$$z_0, \vartheta z_0, \vartheta^2 z_0, \ldots, \vartheta^{k-1} z_0$$

zu. Einer der Terme dieser Reihe reducirt sich auf z_0; nehmen wir an, es sei

$$\vartheta^k z_0 = z_0 \text{ oder } \vartheta^{k-1} \vartheta z_0 = z_0,$$

so ergiebt sich

$$z_0 = \vartheta^{k-1} z_i.$$

Jede der beiden Wurzeln z_0 und z_i lässt sich folglich rational durch die andere ausdrücken.

Daraus geht hervor, dass die bekannten Grössen in beiden Fällen dieselben sind, man mag z_0 oder z_i adjungirt haben. Das System Γ_i, welches der Gleichung $f(x) = 0$ eigen ist, nachdem man z_i adjungirt hat, ist also dasselbe wie das System Γ, welches der Gleichung eigen ist, nachdem man z_0 adjungirt hat. Da nun die Systeme Γ, Γ_i durch

$$\begin{array}{llll} 1, S_1, & S_2, & \ldots, & S_{\mu-1}, \\ 1, T_i S_1 T_i^{-1}, & T_i S_2 T_i^{-1}, & \ldots, & T_i S_{\mu-1} T_i^{-1} \end{array}$$

dargestellt werden können, so sieht man, dass das System Γ sich nicht ändert, wenn man seine Substitutionen zur Rechten mit T_i und zur Linken mit T_i^{-1} multiplicirt, was mit der Ausführung der Substitution T_i in den Cyclen der Substitutionen von Γ gleichbedeutend ist.

Endlich ist jede Substitution von G von der Form

$$U = T_k S_h,$$

und dies liefert

$$U^{-1} = S_h^{-1} T_k^{-1},$$

so dass

$$U S_i U^{-1} = T_k S_h S_i S_h^{-1} T_k^{-1}$$

ist. Will man also die Substitution U in den Cyclen der Substitutionen von Γ ausführen, so genügt es, in diesen Cyclen zuerst die Substitution S_h, dann die Substitution T_k zu vollziehen. Die erste Operation lässt Γ offenbar unverändert, da S_h diesem Systeme angehört. Ausserdem haben wir eben bewiesen, dass auch die zweite Operation keine Aenderung des Systems Γ zur Folge haben kann. Dieses System bleibt also unverändert, wenn man in den Cyclen aller seiner Substitutionen die Substitution U ausführt.

Zusatz. — Wenn die Hilfsgleichung von der Form $z^p = A$ ist, und wenn die p^{ten} Wurzeln der Einheit sich unter den zuvor adjungirten Grössen befinden, so sind die Bedingungen des vorhergehenden Lehrsatzes erfüllt.

570. Lehrsatz V. — Wenn das der Gleichung $f(x) = 0$ eigene conjugirte System G sich auf ein System niedrigerer Ordnung Γ reducirt, dadurch dass man der Gleichung alle Wurzeln einer irreductibelen Hilfsgleichung m^{ten} Grades $\varphi(z) = 0$ adjungirt, so erleidet das System Γ keine Aenderung, wenn man in den Cyclen aller seiner Substitutionen irgend eine Substitution von G ausführt*).

Es sei Z eine rationale Function der m Wurzeln

(1). $$z_0\,,\ z_1\,,\ z_2\,,\ \ldots\,,\ z_{m-1}$$

der Hilfsgleichung, und diese Function sei so beschaffen, dass die

$$M = 1\,.\,2\,.\,3\,\ldots\,m$$

Functionen, welche sich daraus durch die Substitutionen ergeben, verschiedene Werthe haben. Ausserdem seien

$$\mathfrak{F}(Z) = 0$$

die Gleichung M^{ten} Grades, welche die M Werthe von Z zu Wurzeln hat, $F(Z)$ ein irreductibeler Divisor von $\mathfrak{F}(Z)$ und

(2). $$Z_0\,,\ Z_1\,,\ Z_2\,,\ \ldots\,,\ Z_{\mu-1}$$

die μ Wurzeln der Gleichung

(3). $$F(Z) = 0.$$

Die Grössen (2) sind rationale Functionen der Grössen (1), und umgekehrt können letztere rational durch die ersteren ausgedrückt werden. Adjungirt man also die einen, so werden dadurch auch die anderen adjungirt. Folglich muss das der vorgelegten Gleichung eigene System G unserer Voraussetzung nach sich reduciren, wenn man die Wurzeln der Gleichung (3) adjungirt. Diese Wurzeln kann man aber rational durch irgend eine derselben ausdrücken. Mithin werden alle Wurzeln adjungirt, sobald dies mit einer Wurzel geschieht, und man befindet sich dann in den Bedingungen des Lehrsatzes IV.

---

*) Dieser Satz unterscheidet sich im Grunde nicht von dem Satze III der Arbeit von Galois. Unter dem Titel: Satz III hatte Galois anfangs den Zusatz zu unserem Lehrsatze IV mit einem Beweise gegeben. Später entfernte er dies Alles und setzte dafür die schliesslich von ihm angenommene Fassung.

571. Lehrsatz VI. — Es seien G das der Gleichung

$$(1).\qquad f(x) = 0$$

eigene conjugirte System und

$$(2).\qquad z_0 = \mathfrak{F}(x_0, x_1, x_2, \ldots, x_{n-1})$$

eine rationale Function der n Wurzeln

$$x_0, x_1, x_2, \ldots, x_{n-1},$$

deren numerischer Werth gegenwärtig nicht bekannt ist. Das System Γ, welches der Gleichung eigen ist, nachdem man derselben diesen numerischen Werth adjungirt hat, besteht aus denjenigen der Substitutionen von G, welche den numerischen Werth der Function $\mathfrak{F}$ nicht verändern.

Die Bedingungen dieses Lehrsatzes lassen sich ohne Weiteres auf diejenigen des Satzes III zurückführen. Wir vollziehen in dem Ausdrucke

$$z - \mathfrak{F}(x_0, x_1, x_2, \ldots, x_{n-1})$$

alle Substitutionen der Wurzeln x und bilden das Produkt $\Phi(z)$ aller so erhaltenen Resultate. Die Coefficienten des Polynoms $\Phi(z)$ werden symmetrische Functionen der Wurzeln x, folglich in rationaler Form bekannt sein. Zerlegen wir dieses Polynom in seine irreductibelen Factoren und bezeichnen einen dieser Factoren, die für $z = z_0$ verschwinden, mit $\varphi(z)$, so befinden wir uns in dem Falle, in welchem man der vorgelegten Gleichung die Wurzel z_0 der irreductibelen Gleichung

$$(3).\qquad \varphi(z) = 0$$

adjungirt.

Es seien, wie im Lehrsatze III,

$$V_0, V_1, \ldots, V_{\nu-1}$$

die ν Wurzeln der Resolvente

$$(4).\qquad F(V) = 0,$$

welche gegenwärtig irreductibel ist. Da die Wurzeln x sich rational durch irgend eine der Wurzeln V ausdrücken lassen, so setzen wir, wie früher,

$$x_0 = \psi_0(V_0),\ x_1 = \psi_1(V_0), \ldots, x_{n-1} = \psi_{n-1}(V_0);$$

dann geht die Formel (2) über in

$$z_0 = \mathfrak{F}[\psi_0(V_0), \psi_1(V_0), \ldots, \psi_{n-1}(V_0)] = \Psi(V_0),$$

und man kann bewirken (No. 182), dass Ψ eine ganze Function sei, deren Grad kleiner als ν ist. Die Gleichung

(5). $$\Psi(V) - z_0 = 0$$

lässt jetzt die Wurzel V_0 der Gleichung (4) zu. Es seien

(6). $$V_0\,,\; V_1\,,\; \ldots\,,\; V_{\mu-1}$$

die den Gleichungen (4) und (5) gemeinschaftlichen μ Wurzeln, und es werde

$$\lambda(V, z_0) = (V - V_0)(V - V_1)\ldots(V - V_{\mu-1})$$

gesetzt. Nachdem man z_0 adjungirt hat, sind die Coefficienten der Gleichung

(7). $$\lambda(V, z_0) = 0$$

rational. Wir behaupten nun, diese Gleichung (7) sei irreductibel. Wäre nämlich das Gegentheil der Fall, und $\omega(V, z_0)$ der irreductibele Divisor von $\lambda(V, z_0)$, welcher für $V = V_0$ verschwindet, so hätte man (Lehrsatz III)

$$F(V) = \omega(V, z_0)\,\omega(V, z_1)\ldots\omega(V, z_{p-1}),$$

wo $z_1\,, z_2\,, \ldots\,, z_{p-1}$ von z_0 verschiedene Wurzeln der Gleichung (2) sind. Die Gleichung

$$\omega(V, z_0) = 0$$

wird nur einen Theil der Wurzeln (6) zulassen, und eine dieser Wurzeln, z. B. V_1, wird einer Gleichung wie

(8). $$\omega(V, z_1) = 0$$

genügen müssen. Wird $\Psi(V) - z$ so lange durch $\omega(V, z)$ dividirt, bis der Rest $\Theta(V, z)$ von einem niedrigeren Grade als der Divisor ist, so hat man, wenn $\Pi(V, z)$ den Quotienten dieser Division bezeichnet,

$$\Psi(V) - z = \omega(V, z)\,\Pi(V, z) + \Theta(V, z).$$

Der Voraussetzung nach ist $\Psi(V) - z_0$ durch $\lambda(V, z_0)$, also auch durch $\omega(V, z_0)$ theilbar; folglich muss der Rest $\Theta(V, z)$ der vorigen Division sich für $z = z_0$ identisch auf Null reduciren. Durch ein bereits angewandtes Schlussverfahren ergiebt sich dann, dass ebenderselbe Rest für $z = z_1$ Null ist, und man hat

$$\Psi(V) - z_1 = \omega(V, z_1)\,\Pi(V, z_1).$$

Nun haben wir vorausgesetzt, V_1 sei eine Wurzel der Gleichung (8); es ist daher

$$\Psi(V_1) = z_1,$$

und dies ist unmöglich, da V_1 Wurzel der Gleichung (5), und z_1 von z_0 verschieden ist.

Wir sehen somit, dass die Gleichung (7) irreductibel ist, so dass dieselbe die resolvirende Gleichung wird, nachdem die Wurzel z_0 adjungirt worden ist. Das der vorgelegten Gleichung eigene conjugirte System besteht dann aus den μ Substitutionen, die man dadurch ausführt, dass man in der Permutation der Wurzeln

$$\psi_0(V_0)\,,\ \psi_1(V_0)\,,\ \ldots\,,\ \psi_{n-1}(V_0)$$

V_0 durch jede der Grössen (6) ersetzt.

Ausserdem sind die Grössen (6) diejenigen Wurzeln der Gleichung (5), welche der ursprünglichen Resolvente angehören. Die erwähnten Substitutionen sind also diejenigen, durch welche der numerische Werth z_0 der Function $\mathfrak{F}(x_0\,,\,x_1\,,\,\ldots\,,\,x_{n-1})$ keine Aenderung erleidet.

572. Lehrsatz VII. — Die Ordnung des einer Gleichung $f(x) = 0$ eigenen conjugirten Systems G sei $\nu = \mu p$, wo p eine Primzahl ist. Kann man aus μ Substitutionen von G ein conjugirtes System Γ bilden, welches unverändert bleibt, wenn man in den Cyclen aller seiner Substitutionen die verschiedenen Substitutionen von G ausführt, so genügt es, um Γ zu dem der vorgelegten Gleichung eigenen Systeme zu machen, die p^{te} Wurzel aus einer gewissen rationalen Grösse zu ziehen, und diese Wurzel der Gleichung zu adjungiren. Es wird dabei vorausgesetzt, dass die p^{ten} Wurzeln der Einheit zu den bereits zuvor adjungirten Grössen gehören.

Es seien

$$(1).\qquad 1\,,\ S_1\,,\ S_2\,,\ \ldots\,,\ S_{\mu-1}$$

die Substitutionen des Systems Γ, und T eine Substitution von G, welche Γ nicht angehört. Der Voraussetzung nach ist für jeden Werth von i

$$(2).\qquad TS_iT^{-1} = S_j,$$

wo j ein passend gewählter Index ist. Wenn das System der Potenzen von T

$$(3).\qquad 1\,,\ T\,,\ T^2,\ \ldots\,,\ T^{t-1},$$

dessen Ordnung t sein möge, ausser der Einheit einige Substi-

tutionen mit dem Systeme (1) gemeinschaftlich hat, so sei T^α die kleinste in (1) enthaltene Potenz von T. Werden die Substitutionen (1) mit

$$1\,,\,T\,,\,T^2,\,\ldots\,,\,T^{\alpha-1}$$

multiplicirt, so erhält man die $\mu\alpha$ Produkte

$$(4).\quad \begin{cases} 1 \quad , S_1 \quad , \ldots , S_{\mu-1}, \\ T \quad , TS_1 \quad , \ldots , TS_{\mu-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots , \\ T^{\alpha-1} , T^{\alpha-1}S_1 , \ldots , T^{\alpha-1}S_{\mu-1}. \end{cases}$$

Diese Produkte sind von einander verschieden; denn hätte man

$$T^i S_g = T^{i+j} S_h,$$

so würde sich

$$T^j = S_g S_h^{-1}$$

ergeben, und dies kann nicht der Fall sein, da $S_g S_h^{-1}$ dem Systeme (1) angehört, T^j aber nicht (es ist $j < \alpha$). Ferner kann das Produkt von irgend zwei Substitutionen (4) mittels der Formel (2) auf die Form

$$T^{g\alpha+h} S_k \text{ oder } T^h S_k$$

gebracht werden, wo $h < \alpha$ ist, und dieses Produkt $T^h S_k$ ist selbst eine der Substitutionen (4). Letztere bilden daher ein conjugirtes System der Ordnung $\mu\alpha$. Ausserdem sind sie in dem Systeme G enthalten, dessen Ordnung μp ist. Folglich ist μp durch $\mu\alpha$ und p durch α theilbar, und da p eine Primzahl ist, so muss $\alpha = 1$ oder $= p$ sein. Wenn $\alpha = 1$ ist, so gehört die Substitution T der Voraussetzung zuwider dem Systeme G an. Es ist also $\alpha = p$. Dann enthält aber das System (4) μp Substitutionen und ist folglich nichts Anderes, als das System G selbst. Die in Γ enthaltenen Potenzen von T sind daher

$$1\,,\,T^p,\,T^{2p},\,\ldots\,,\,T^{(k-1)p},$$

und man hat

$$T^{kp} = 1.$$

Ausserdem ist offenbar

$$(k-1)p = \text{ oder } < t-1\,,\; kp = qt,$$

wo q eine ganze Zahl ist. Dies erfordert, dass $q = 1$ sei, so dass die Ordnung der Substitution T nothwendig gleich p oder gleich einem Vielfachen von p ist.

Dies vorausgesetzt, sei Θ eine rationale Function der n Wurzeln $x_0, x_1, x_2, \ldots, x_{n-1}$ von $f(x) = 0$, die so beschaffen ist, dass die durch die Substitutionen daraus hervorgehenden $1.2.3\ldots n$ Functionen ungleiche numerische Werthe haben. Wir führen in dieser Function die μ Substitutionen (1) von Γ aus und bezeichnen die erhaltenen Resultate mit

$$(5). \qquad \Theta_0, \Theta_1, \Theta_2, \ldots, \Theta_{\mu-1}.$$

Endlich nehmen wir eine rationale und symmetrische Function ϑ der μ Grössen (5); man kann z. B.

$$(6). \qquad \vartheta = (\Theta - \Theta_0)(\Theta - \Theta_1) \ldots (\Theta - \Theta_{\mu-1})$$

machen, wo Θ eine unbestimmte Grösse bezeichnet.

Die Function ϑ erleidet durch die Substitutionen von Γ keine Veränderung; aber jede andere Substitution bringt eine Aenderung in ihr hervor. Wir führen in dieser Function die Potenzen der Substitution T, nämlich:

$$1, T, T^2, \ldots, T^{p-1}$$

aus und bezeichnen das durch die Substitution T^i erhaltene Resultat mit ϑ_i. Ferner stellen wir durch α eine Wurzel der Gleichung

$$\frac{x^p - 1}{x - 1} = 0$$

dar und setzen

$$(\vartheta_0 + \alpha\vartheta_1 + \alpha^2\vartheta_2 + \cdots + \alpha^{p-1}\vartheta_{p-1})^p = \Omega.$$

Die Substitution T, deren Wirksamkeit darin besteht, die Grössen

$$\vartheta_0, \vartheta_1, \vartheta_2, \ldots, \vartheta_{p-1}$$

cyclisch zu versetzen, lässt die Function Ω offenbar ungeändert. Ebenso wenig bringen die Substitutionen von Γ eine Aenderung in Ω hervor; denn es ist

$$\vartheta_i = T^i . \vartheta_0,$$

und daraus folgt durch Ausführung einer Substitution S

$$S_j\vartheta_i = S_j T^i \vartheta_0 = T^i S_k \vartheta_0 = T^i \vartheta_0 = \vartheta_i.$$

Wir sehen somit, dass alle Substitutionen des der vorgelegten Gleichung gegenwärtig eigenen Systems G die Function Ω unverändert lassen. Daraus ergiebt sich, dass der Werth von Ω bekannt ist. Wird also die Wurzelgrösse

$$\sqrt[p]{\Omega}$$

der Gleichung adjungirt, so ist auch die Function

$$\vartheta_0 + \alpha\vartheta_1 + \alpha^2\vartheta_2 + \cdots + \alpha^{p-1}\vartheta_{p-1} = \sqrt[p]{\Omega}$$

bekannt.

Die einzigen Substitutionen, welche keine Aenderung dieser Function zur Folge haben, sind diejenigen von Γ. Adjungirt man also $\sqrt[p]{\Omega}$, so wird (Lehrsatz VI) Γ das der Gleichung eigene conjugirte System.

573. Die im Vorhergehenden hergeleiteten Sätze setzen uns in den Stand, die Lösung der Aufgabe in Angriff zu nehmen:

In welchem Falle ist eine Gleichung durch Wurzelgrössen lösbar?

Zu diesem Zwecke bemerkt Galois, dass nach Auflösung einer Gleichung eine beliebige Function der Wurzeln bekannt ist, selbst wenn dieselbe durch keine Substitution ungeändert gelassen wird. Das der Gleichung eigene conjugirte System enthält dann also nur die der Einheit gleiche identische Substitution.

Die Lösung der Aufgabe, deren Gegenstand die Auflösung einer Gleichung ist, muss also darin bestehen, dass man die Ordnung des der Gleichung eigenen conjugirten Systems immer mehr erniedrigt.

„Verfolgen wir," sagt Galois, „die Reihe der in dieser „Lösung möglichen Operationen, indem wir die Ausziehung jeder „Wurzel, deren Exponent eine Primzahl ist, als besondere Ope-„ration ansehen.

„Adjungiren wir der Gleichung die erste in der Lösung aus-„gezogene Wurzel, so können zwei Fälle eintreten: Entweder „wird die Ordnung des der Gleichung eigenen conju-„girten Systems verkleinert*), oder diese Wurzelausziehung „ist nur eine einfache Vorbereitung, und das der Gleichung „eigene System bleibt unverändert.

„Immer muss aber, wenn die Gleichung lösbar sein soll, „die Ordnung des ihr eigenen conjugirten Systems nach einer „gewissen endlichen Anzahl von Wurzelausziehungen kleiner ge-„worden sein.

„Hätten wir, hier angelangt, mehrere Wege, die Ordnung

---

*) Die unbedeutenden Aenderungen, die hier durch den ausschliesslichen Gebrauch der Systeme von Substitutionen, statt der Permutationsgruppen, erfordert werden, sind durch fette Schrift angedeutet.

„des der vorgelegten Gleichung eigenen Systems durch „eine einfache Wurzelausziehung zu verringern, so würde für das „Folgende von allen einfachen Wurzelgrössen, die so beschaffen „sind, dass die Kenntniss einer jeden derselben die Ordnung „des der Gleichung eigenen Systems erniedrigt, eine Wur- „zelgrösse von einem möglichst niedrigen Grade zu betrachten „sein.

„Es sei p die Primzahl, welche diesen kleinsten Grad darstellt, „so dass durch Ausziehung einer p^{ten} Wurzel die Ordnung des „der Gleichung eigenen Systems verringert wird.

„Wir können immer voraussetzen, wenigstens in Betreff des „der Gleichung eigenen Systems, dass sich unter den der „Gleichung schon zuvor adjungirten Grössen eine p^{te} Wurzel der „Einheit befindet. Denn da dieser Ausdruck durch Ausziehung „von Wurzeln erhalten wird, deren Grade kleiner als p sind, so „wird durch die Kenntniss desselben das der Gleichung eigene „System in Nichts geändert.“

Es tritt hier die volle Bedeutung der Lehrsätze III und IV zu Tage. Unter der gemachten Voraussetzung reducirt sich das der Gleichung eigene conjugirte System, welches gegenwärtig G ist, auf ein System niedrigerer Ordnung Γ. Daraus folgt mit Beziehung auf die Lehrsätze III und IV (Zusatz), dass die Ordnung von Γ ein Divisor der Ordnung von G ist, und dass dieses System unverändert bleibt, wenn man in den Cyclen aller seiner Substitutionen irgend eine der Substitutionen von G ausführt. Ist umgekehrt (Lehrsatz VII) G das der Gleichung eigene System $(\mu p)^{\text{ter}}$ Ordnung, und lässt sich ein in G enthaltenes System μ^{ter} Ordnung Γ ermitteln, welches unverändert bleibt, wenn man in den Cyclen aller seiner Substitutionen die Substitutionen von G ausführt, so wird Γ das der Gleichung eigene System, dadurch dass man eine p^{te} Wurzel auszieht und diese Wurzel adjungirt.

Diese von Galois entdeckten Sätze, die wir im Vorstehenden vollständig und streng bewiesen haben, geben somit die Bedingung an, die erforderlich und hinreichend ist, damit die Ordnung des der Gleichung eigenen conjugirten Systems erniedrigt werde.

Hat man diese Ordnung auf die angegebene Weise einmal erniedrigt, so kann man auf das neue conjugirte System wieder das dargelegte Schlussverfahren anwenden. Dies System muss

sich ebenso reduciren lassen, u. s. w, und man muss schliesslich zu einem Systeme gelangen, welches nur die der Einheit gleiche Substitution enthält.

574. Es ist leicht, wie Galois bemerkt hat, dies Verfahren in der bekannten Auflösung der allgemeinen Gleichung vierten Grades zu beobachten.

Die Wurzeln seien

$$a, b, c, d.$$

Das der Gleichung eigene System G ist hier das System der $1 . 2 . 3 . 4 = 24$ Substitutionen der Wurzeln, und man erhält es (No. 431) durch Multiplication der vier Systeme

$$\begin{array}{l} 1 , (a , b) (c , d) , \\ 1 , (a , c) (b , d) , \\ 1 , (b , c , d) , (b , d , c) , \\ 1 , (b , c). \end{array}$$

Die in Rede stehende Gleichung wird mittels einer Gleichung dritten Grades gelöst, welche die Ausziehung einer Quadratwurzel erfordert. Mit dieser Wurzel hat man naturgemäss zu beginnen. Wird dieselbe der vorgelegten Gleichung adjungirt, so reducirt sich (Lehrsatz VII) die Ordnung des der Gleichung eigenen Systems auf 12, und dies System wird gleich dem Produkte der drei Systeme

$$\begin{array}{l} 1 , (a , b) (c , d) , \\ 1 , (a , c) (b , d) , \\ 1 , (b , c , d) , (b , d , c). \end{array}$$

Jetzt reducirt man durch Ausziehung einer Kubikwurzel die Ordnung des der Gleichung eigenen Systems auf 4; dasselbe ist das Produkt der beiden Systeme

$$\begin{array}{l} 1 , (a , b) (c , d) , \\ 1 , (a , c) (b , d) . \end{array}$$

Die Ausziehung einer Quadratwurzel erniedrigt sodann die Ordnung des Systems auf 2, und das System wird auf diese Weise

$$1 , (a , b) (c , d).$$

Endlich wird durch Ausziehung einer letzten Quadratwurzel das der Gleichung eigene System auf die Einheit reducirt, und dann ist die Gleichung aufgelöst.

Fortsetzung der Untersuchungen von Galois. — Anwendung auf die irreductibelen Gleichungen, deren Grad eine Primzahl ist.

575. Die Anwendungen der dargelegten Theorie bieten noch viele Schwierigkeiten dar*). Wir werden uns darauf beschränken, zu betrachten, wie Galois seine Theorie auf die irreductibelen Gleichungen anwendet, deren Grad eine Primzahl ist.

Hilfssatz. — Eine irreductibele Gleichung, deren Grad eine Primzahl ist, kann nicht dadurch reductibel werden, dass man ihr eine Wurzelgrösse adjungirt, deren Exponent vom Grade der Gleichung verschieden ist.

Wir nehmen an, die irreductibele Gleichung

$$(1). \qquad f(x) = 0,$$

deren Grad n eine Primzahl ist, werde reductibel, wenn man ihr eine Wurzelgrösse adjungirt. Da die Ausziehung einer Wurzel zusammengesetzten Grades sich darauf zurückführen lässt, nach einander mehrere Wurzeln auszuziehen, deren Grade Primzahlen sind, so darf der Exponent der in Rede stehenden Wurzel als Primzahl vorausgesetzt werden. Nur muss man, wenn die Grösse, aus der diese Wurzel gezogen werden soll, nicht zu den gegenwärtig bekannten Grössen gehört, dieselbe als der Gleichung adjungirt ansehen.

Dies vorausgesetzt, sei m die kleinste Primzahl von der Beschaffenheit, dass die Gleichung (1) reductibel wird, wenn man eine Wurzel einer Gleichung von der Form

$$(2). \qquad z^m = A$$

adjungirt; darin bedeutet A eine bekannte Grösse, oder eine Grösse, welche, der Gleichung adjungirt, keine Reduction zur Folge hat. Die Wurzeln der Gleichung

$$(3). \qquad z^m = 1$$

können als zu den bekannten Grössen gehörig angesehen werden, insofern sie durch Ausziehung von Wurzeln erhalten wer-

*) In der letzten Zeit hat Jordan neue Untersuchungen über diesen Gegenstand der Akademie der Wissenschaften eingereicht. Seine Arbeit ist aber noch nicht veröffentlicht worden.

den, deren Grade kleiner als m sind, und insofern ihre Kenntniss unserer Voraussetzung nach nicht dazu genügt, die Reduction der Gleichung auszuführen.

Bezeichnen r eine Wurzel der Gleichung (2) und α eine primitive Wurzel der Gleichung (3), so sind

$$r\ ,\ \alpha r\ ,\ \alpha^2 r\ ,\ \ldots\ ,\ \alpha^{m-1} r$$

die Wurzeln von (2). Wenn jetzt die Gleichung (1) reducirt wird, dadurch dass man ihr r adjungirt, so sei $\varphi(x, r)$ der irreductibele Divisor von $f(x)$, welcher den kleinsten Grad hat. Dann ist das Polynom $f(x)$ durch jede der Functionen

$$\varphi(x, r)\ ,\ \varphi(x, \alpha r)\ ,\ \ldots\ ,\ \varphi(x, \alpha^{m-1} r)$$

theilbar. Das Produkt dieser Divisoren lässt sich als symmetrische Function der Wurzeln der Gleichung (2) rational durch die bekannten Grössen ausdrücken. Ausserdem kann dieses Produkt nur für die Werthe von x verschwinden, welche der Gleichung (1) genügen. Da nun diese Gleichung irreductibel ist, so muss das in Rede stehende Produkt eine Potenz von $f(x)$ sein, und man hat

$$(4). \qquad [f(x)]^q = \varphi(x, r)\ \varphi(x, \alpha r)\ \ldots\ \varphi(x, \alpha^{m-1} r).$$

Wenn die beiden Gleichungen

$$\varphi(x, \alpha^i r) = 0\ ,\ \varphi(x, \alpha^j r) = 0$$

eine Wurzel gemeinschaftlich haben, so haben sie alle ihre Wurzeln gemeinschaftlich. Denn wenn das Gegentheil der Fall wäre, so würden die ersten Glieder dieser Gleichungen einen in Beziehung auf die bekannten Grössen rationalen gemeinschaftlichen Divisor $\psi(x, r)$ haben, und $\varphi(x, r)$ wäre nicht der Divisor niedrigsten Grades von $f(x)$.

Zieht man dann die q^{te} Wurzel aus beiden Gliedern der Formel (4), so erhält man ein Resultat von der Form

$$(5). \qquad f(x) = \varphi(x, r)\ \varphi(x, \alpha r)\ \varphi(x, \beta r)\ \ldots\ \varphi(x, \varepsilon r),$$

wo $\alpha, \beta, \ldots, \varepsilon$ Wurzeln der Gleichung (3) bezeichnen. Da aber der Grad von $f(x)$ eine Primzahl ist, so kann die Formel (5) nur statthaben, wenn die Polynome φ vom ersten Grade sind, und die Formel (4) zeigt, dass m durch n theilbar ist. Nun ist m eine Primzahl; man hat somit $m = n$.

Zusatz. — Eine irreductibele Gleichung, deren Grad eine Primzahl ist, kann nicht reductibel werden, wofern das ihr eigene conjugirte System sich nicht

auf die eine der Einheit gleiche Substitution reducirt.

Wenn die vorgelegte Gleichung reducirt wird, so zerfällt ihr erstes Glied nach dem eben bewiesenen Hilfssatze in lineare Factoren; sie wird somit aufgelöst.

576. Wir haben jetzt noch die Lehrsätze mitzutheilen, durch welche Galois die Bedingung ausgedrückt hat, unter welcher die Gleichungen, deren Grad eine Primzahl ist, aufgelöst werden können.

Lehrsatz I. — Wenn eine irreductibele Gleichung $f(x) = 0$, deren Grad n eine Primzahl ist, durch Wurzelgrössen gelöst werden kann, so lassen sich ihre n Wurzeln in der Weise durch x_z [der Index z muss nach dem Modul n genommen, also auf eine der Zahlen $0, 1, 2 \ldots, (n-1)$ reducirt werden] darstellen, dass das der Gleichung gegenwärtig eigene conjugirte System nur lineare und ganze Substitutionen, d. h. Substitutionen von der Form $\binom{az+b}{z}$ enthält, wo a und b Constante sind.

Das der Gleichung eigene conjugirte System reducirt sich der Voraussetzung nach auf die Einheit, wenn man der Gleichung der Reihe nach gewisse Wurzelgrössen adjungirt, und diese Gleichung bleibt nach dem vorhergehenden Hilfssatze so lange irreductibel, bis die letzte Wurzelgrösse adjungirt worden ist. Diese letzte Operation, die sich auf eine Wurzel mit dem Exponenten n bezieht, vollführt nicht nur die Reduction, sondern auch die Auflösung der Gleichung (No. 575) und theilt nach dem Lehrsatze der No. 568 die Ordnung des der Gleichung eigenen conjugirten Systems durch n.

Das der Gleichung eigene System hat also, unmittelbar bevor es auf die Einheit reducirt wird, die Ordnung n. Wenn aber n eine Primzahl und die Ordnung eines auf n Buchstaben bezüglichen conjugirten Systems gleich n ist, so besteht das System aus den Potenzen einer cyclischen Substitution n^{ter} Ordnung (No. 414, Zusatz III). Das vorletzte der Gleichung eigene System wird also durch die Potenzen einer Substitution gebildet, die durch

$$\binom{z+1}{z}$$

dargestellt wird, wenn die n Indices passend unter die n Wurzeln vertheilt sind. Mit anderen Worten, das in Rede stehende System besteht aus den n linearen Substitutionen von der Form

$$\begin{pmatrix} z + b \\ z \end{pmatrix},$$

wo man b n den Zahlen

$$0, 1, 2, \ldots, (n-1)$$

nach dem Modul n congruente Werthe ertheilen muss; die Indices werden, wie wir schon bemerkt haben, in Beziehung auf denselben Modul genommen.

Dies vorausgesetzt, behaupten wir, dass, wenn man von diesem vorletzten zu dem der Gleichung gegenwärtig eigenen conjugirten Systeme emporsteigt, in jedem Systeme nur lineare und ganze Substitutionen von der Form

$$\begin{pmatrix} az + b \\ z \end{pmatrix}$$

angetroffen werden. Da dieser Satz für das vorletzte System bereits feststeht, so haben wir nur darzuthun, dass, wenn derselbe für irgend ein System Γ statt hat, er auch für das in der Reihenfolge der Reductionen Γ unmittelbar vorhergehende System G gültig ist. Zu diesem Zwecke bemerken wir, dass, wenn Γ auch nicht das vorletzte System ist, es doch dessen Substitutionen enthält. Es sei S_i eine derselben, so hat man

$$S_i = \begin{pmatrix} z + \beta \\ z \end{pmatrix},$$

wo β eine der Zahlen $1, 2, 3, \ldots, (n-1)$ ist. Bezeichnet jetzt T irgend eine der Substitutionen von G, so ist nach dem Lehrsatze der No. 569 für jeden Werth von i

$$TS_iT^{-1} = S_j \text{, oder } TS_i = S_jT,$$

wo S_j eine Substitution von Γ ist. Diese Formel drückt aus, dass S_j ähnlich S_i, folglich eine cyclische Substitution ist. Nun enthält das System Γ unserer Voraussetzung nach nur lineare und ganze Substitutionen. Daraus folgt, dass dieses System nicht zwei cyclische Substitutionen n^{ter} Ordnung S_i und S_j enthalten kann, von denen die eine nicht eine Potenz der andern ist; denn sonst würde es die n^2 Produkte von der Form $S_i^\alpha S_j^\beta$ enthalten, die sämmtlich verschieden sein würden, und dies ist aus dem

Grunde unmöglich, weil die Gesammtzahl der linearen Substitutionen nur $n(n-1)$ ist. S_j ist also eine Potenz von S_i, und man hat

$$S_j = \begin{pmatrix} z + a \\ z \end{pmatrix}.$$

Setzen wir

$$T = \begin{pmatrix} F(z) \\ z \end{pmatrix},$$

so ist

$$TS_i = \begin{pmatrix} F(z+\beta) \\ z \end{pmatrix}, \quad S_j T = \begin{pmatrix} F(z) + a \\ z \end{pmatrix},$$

folglich

$$F(z+\beta) = F(z) + a.$$

Ersetzt man z der Reihe nach durch

$$z + \beta, z + 2\beta, \ldots, z + Z\beta,$$

so folgt

$$\begin{aligned} F(z + 2\beta) &= F(z+\beta) + a = F(z) + 2a, \\ F(z + 3\beta) &= F(z+\beta) + 2a = F(z) + 3a, \\ &\ldots\ldots\ldots\ldots, \\ F(z + Z\beta) &= F(z+\beta) + (Z-1)a = F(z) + Za. \end{aligned}$$

Wird endlich in der letzten dieser Formeln

$$\beta = 1, z = 0, F(0) = b$$

gesetzt, so erhält man

$$F(Z) = aZ + b,$$

wo a und b Constanten sind. Das System G enthält also nur Substitutionen von der Form

$$\begin{pmatrix} az + b \\ z \end{pmatrix}.$$

Dies gilt im Besonderen auch für das der Gleichung gegenwärtig eigene System.

577. Lehrsatz II. — Wenn umgekehrt das der irreductibelen Gleichung $f(x) = 0$, deren Grad n eine Primzahl ist, gegenwärtig eigene System G nur Substitutionen von der Form

$$\begin{pmatrix} az + b \\ z \end{pmatrix}$$

enthält, so ist die Gleichung algebraisch auflösbar.

Es seien α eine Wurzel der Gleichung

$$(1).\qquad \frac{x^n-1}{x-1}=0$$

und r eine primitive Wurzel der Primzahl n. Ausserdem setzen wir

$$(2).\begin{cases} X_1 &= (x_0+\alpha\, x_1+\alpha^2 x_2+\cdots+\alpha^{n-1}x_{n-1})^n,\\ X_r &= (x_0+\alpha\, x_r+\alpha^2 x_{2r}+\cdots+\alpha^{n-1}x_{(n-1)r})^n,\\ X_{r^2} &= (x_0+\alpha\, x_{r^2}+\alpha^2 x_{2r^2}+\cdots+\alpha^{n-1}x_{(n-1)r^2})^n,\\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot,\\ X_{r^{n-2}} &= (x_0+\alpha\, x_{r^{n-2}}+\alpha^2 x_{2r^{n-2}}+\cdots+\alpha^{n-1}x_{(n-1)r^{n-2}})^n. \end{cases}$$

Jede Substitution des Systems G ist das Produkt einer Potenz der Substitution

$$(3).\qquad \begin{pmatrix} z+1 \\ z \end{pmatrix}$$

in eine Potenz der Substitution

$$(4).\qquad \begin{pmatrix} rz \\ z \end{pmatrix}.$$

Die Grössen

$$(5).\qquad X_1\,,\; X_r\,,\; X_{r^2}\,,\;\ldots\,,\; X_{r^{n-2}}$$

erleiden durch die Substitution (3) (No. 482) keine Veränderung, werden aber durch die Substitution (4) cyclisch versetzt. Folglich ist jede Function Ξ der Grössen (5), welche die an den Indices der Functionen X vollzogene Substitution (4) ungeändert lässt, eine Function der Wurzeln $x_0\,, x_1\,, \ldots, x_{n-1}$, die durch keine Substitution des Systems G verändert wird. Diese Function Ξ darf daher (No. 566) als eine bekannte rationale Grösse angesehen werden.

Bezeichnet λ eine Wurzel der Gleichung

$$(6).\qquad x^{n-1}-1=0,$$

und macht man im Besonderen

$$(X_1+\lambda\, X_r+\lambda^2 X_{r^2}+\cdots+\lambda^{n-2} X_{r^{n-2}})^{n-1}=\Xi,$$

so ist die Grösse Ξ bekannt; nach Ausziehung einer Wurzel $(n-1)^{\text{ten}}$ Grades kennt man also auch die Grösse

$$X_1+\lambda X_r+\lambda^2 X_{r^2}+\cdots+\lambda^{n-2} X_{r^{n-2}}=\sqrt[n-1]{\Xi}\,.$$

Nimmt man für λ der Reihe nach jede der Wurzeln der Gleichung $x^{n-1}-1=0$, so erhält man $n-1$ Gleichungen, welche die Grössen (5) kennen lehren. Zieht man sodann die n^{te} Wur-

zel aus den Gleichungen (2), so ergeben sich $n-1$ Gleichungen ersten Grades, welche, da noch die Summe der Wurzeln x bekannt ist, diese Wurzeln bestimmen.

Die vorgelegte Gleichung ist somit unter der gemachten Voraussetzung algebraisch lösbar.

578. Mittels der vorhergehenden Sätze hat Galois die Bedingung, unter welcher eine irreductibele Gleichung, deren Grad eine Primzahl ist, sich algebraisch auflösen lässt, folgendermassen aussprechen können:

Lehrsatz III. — Damit eine irreductibele Gleichung, deren Grad eine Primzahl ist, durch Wurzelgrössen gelöst werden könne, ist erforderlich und hinreichend, dass die Resolvente von Lagrange eine rationale Wurzel habe.

Die Wurzeln dieser Resolvente vom Grade $1 \,.\, 2 \,.\, 3 \ldots (n-2)$ sind die verschiedenen Werthe, welche eine symmetrische Function der Grössen (5) der No. 577, z. B. die Function

$$(X-X_1)\,(X-X_r)\ldots(X-X_{r^{n-2}}),$$

wo X eine unbestimmte Grösse bedeutet, in Folge der Substitutionen der Wurzeln x annimmt. Nun lehren die Sätze I und II, dass, wenn die vorgelegte Gleichung gelöst werden kann, diese Grösse, unabhängig von X, bekannt ist. Folglich muss die Resolvente, von der sie abhängt, eine rationale Wurzel haben.

Wenn umgekehrt die Resolvente eine rationale Wurzel besitzt, so ist die vorgelegte Gleichung lösbar. In diesem Falle ist nämlich die eben betrachtete Function, ganz unabhängig von X, bekannt: es ist dies eben die rationale Wurzel der Resolvente. Nun bleibt diese Function nur durch die Substitutionen von der Form $\begin{pmatrix} az+b \\ z \end{pmatrix}$ unverändert. Folglich enthält das der Gleichung eigene System (No. 571) nur solche Substitutionen, und die vorgelegte Gleichung ist (No. 577) lösbar.

579. Die für die Auflösbarkeit der irreductibelen Gleichungen soeben ermittelte Bedingung lässt sich noch auf eine andere Weise aussprechen; dies ist der Gegenstand der folgenden Sätze.

Lehrsatz IV. — Wenn eine irreductibele Gleichung, deren Grad eine Primzahl ist, durch Wurzelgrössen gelöst werden kann, so kann man alle ihre Wurzeln rational durch irgend zwei derselben ausdrücken.

Nach dem Lehrsatze I enthält das der Gleichung gegenwärtig eigene conjugirte System nur Substitutionen von der Form $\begin{pmatrix} az+b \\ z \end{pmatrix}$. Nun versetzt eine solche Substitution, die sich nicht auf die Einheit reducirt, die n Indices, wenn $a=1$, dagegen $n-1$ Indices, wenn a von 1 verschieden ist. Daraus geht hervor, dass, wenn man der Gleichung zwei Wurzeln

$$x_\alpha\ ,\ x_\beta$$

adjungirt, das dieser Gleichung eigene System nur noch die der Einheit gleiche Substitution enthalten kann; denn nach dem Lehrsatze der No. 571 können die Substitutionen dieses Systems die Indices α und β nicht versetzen. Wenn also die Wurzeln x_α und x_β als bekannt angesehen werden, so sind auch alle übrigen in rationaler Form bekannt.

580. Lehrsatz V. — Wenn man umgekehrt alle Wurzeln einer irreductibelen Gleichung, deren Grad eine Primzahl ist, rational durch irgend zwei derselben ausdrücken kann, so ist die Gleichung durch Wurzelgrössen lösbar.

Es seien x_α, x_β zwei beliebige Wurzeln der vorgelegten Gleichung

$$f(x) = 0. \tag{1}$$

Ferner seien G das der Gleichung gegenwärtig eigene System, Γ das System, welches an die Stelle von G tritt, nachdem x_α, aber bevor x_β adjungirt worden ist. Endlich sei

$$F(V) = 0 \tag{2}$$

die irreductibele Gleichung, die wir Resolvente genannt haben, und deren Grad die Ordnung des Systems G ausdrückt.

Die Gleichung (2) wird reductibel, wenn man x_α adjungirt; denn ist V_0 eine ihrer Wurzeln, so kann man x_α rational durch V_0 ausdrücken, und wenn man

$$x_\alpha = \psi(V_0)$$

setzt, so darf (No. 182) ψ als eine ganze Function angesehen werden, deren Grad kleiner, als derjenige von $F(V)$ ist. Die Wurzel V_0 ist also der Gleichung

$$\psi(V) - x_\alpha = 0$$

und der Gleichung (2) gemeinschaftlich; letztere hört folglich auf, irreductibel zu sein. Die Reduction geschieht dann aber durch

Zerlegung von $F(V)$ in p Factoren desselben Grades, wo p ein Divisor des Grades der irreductibelen Hilfsgleichung ist, von welcher die adjungirte Wurzel abhängt. Diese Hilfsgleichung ist hier nichts Anderes, als die vorgelegte Gleichung selbst, und da deren Grad n eine Primzahl ist, so hat man $p = n$. Die Ordnung des Systems Γ ist mithin der n^{te} Theil der Ordnung von G.

Adjungiren wir jetzt die Wurzel x_β. Da die Wurzel x_α gegenwärtig zu den bekannten Grössen gehört, so ist die noch zu adjungirende Grösse x_β Wurzel einer irreductibelen Gleichung

(3).
$$f_1(x, x_\alpha) = 0,$$

deren erstes Glied gleich dem Quotienten $\frac{f(x)}{x - x_\alpha}$, oder gleich einem rationalen Divisor dieses Quotienten ist, und der Voraussetzung nach muss das der Gleichung eigene System, welches gegenwärtig Γ ist, sich auf die Einheit reduciren, wenn man x_β der Gleichung adjungirt. Durch diese Operation wird aber, dem Lehrsatze der No. 568 zufolge, die Ordnung des der Gleichung eigenen Systems durch einen Factor m des Grades der Hilfsgleichung dividirt, der höchstens gleich $n - 1$ ist. Folglich ist Γ von der Ordnung m und G von der Ordnung nm.

Das System G kann keine Substitution enthalten, welche zwei Indices unverrückt stehen lässt. Da sich nämlich die Wurzeln rational durch irgend zwei derselben ausdrücken lassen, so nehmen wir an, es sei

$$x_\gamma = \varphi(x_\alpha, x_\beta), \quad x_\delta = \chi(x_\alpha, x), \quad x_\varepsilon = \omega(x_\alpha, x_\beta), \ldots .$$

Dann sind die Differenzen

$$x_\gamma - \varphi(x_\alpha, x_\beta), \quad x_\delta - \chi(x_\alpha, x_\beta), \ldots$$

bekannt, da sie den Werth Null haben. Wenn nun eine von der Einheit verschiedene Substitution die Indices α und β nicht versetzte, so würde sie einige dieser Differenzen ändern. Eine solche Substitution kann also (No. 566) in G, folglich auch in Γ nicht enthalten sein.

Das System Γ besteht jetzt aus denjenigen der Substitutionen von G, welche den Index α nicht versetzen (No. 571). Ausser der Einheit giebt es also $m - 1$ Substitutionen in G, welche den Index α unbewegt lassen, und da dasselbe für die übrigen Indices gilt, so sieht man, dass $(m-1)n + 1$ oder $mn - (n-1)$ Substitutionen in G enthalten sind, welche die n Indices nicht gleichzeitig

versetzen. Die Anzahl der Substitutionen von G, welche alle Indices versetzen, ist daher gleich $n-1$. Wir behaupten nun, diese Substitutionen seien cyclisch, und es seien die einen Potenzen der andern. Es sei nämlich T eine dieser Substitutionen. Wir zerlegen T in Cyclen, und es ergebe sich

$$T = C_1 \, C_2 \, C_3 \dots .$$

Die Ordnung von T ist ein Divisor von nm. Wenn also T sich nicht auf einen einzigen Cyclus n^{ter} Ordnung reducirt, so muss die Ordnung dieser Substitution gleich einem Divisor d von m sein. Unter der gemachten Voraussetzung versetzt die Substitution T alle Wurzeln. Sie hat also keine Cyclen erster Ordnung. Ausserdem ist sie unregelmässig, da die Anzahl n der Buchstaben eine Primzahl ist. Bezeichnet δ die Ordnung des niedrigsten Cyclus, so lässt die Substitution T^δ wenigstens zwei Buchstaben unversetzt; dieselbe kann somit dem Systeme G nicht angehören, und folglich kann auch T nicht in G enthalten sein.

Das System G enthält also eine cyclische Substitution n^{ter} Ordnung T, und die Potenzen von T sind die einzigen Substitutionen von G, welche alle Indices versetzen. Bezeichnen dann

$$(1). \qquad 1 \, , \, S_1 \, , \, S_2 \, , \dots , \, S_{m-1}$$

die Substitutionen von Γ, so erhält man G, wenn man die Substitutionen (1) zur Rechten, oder zur Linken mit dem aus den Potenzen von T gebildeten conjugirten Systeme

$$(2). \qquad 1 \, , \, T \, , \, T^2 \, , \dots , \, T^{n-1}$$

multiplicirt. Zwei der so erhaltenen Produkte sind in der That verschieden und Substitutionen von G.

Man kann jetzt die Indices $0, 1, 2, \dots$ der Buchstaben x in der Weise vertheilen, dass

$$T = \begin{pmatrix} z+1 \\ z \end{pmatrix}$$

ist. Bezeichnet dann

$$U = \begin{pmatrix} F(z) \\ z \end{pmatrix}$$

irgend eine Substitution von G, so gehört die T ähnliche Substitution UTU^{-1} dem Systeme G an; sie ist ferner cyclisch und fällt nach dem Vorhergehenden mit einer der Potenzen von T zusammen. Man hat also

$$UTU^{-1} = T^a \text{ oder } UT = T^a U,$$

wo a ein passend gewählter Exponent ist. Diese Gleichung drückt aus, dass

$$F(z+1) = F(z) + a$$

ist. Wird hierin z der Reihe nach durch

$$z+1, z+2 \ldots, z+Z$$

ersetzt, so folgt

$$F(z+Z) = F(z) + aZ.$$

Macht man endlich $z = 0$, $F(0) = b$, so erhält man

$$F(Z) = aZ + b;$$

danach enthält das System G nur Substitutionen von der Form $az + b$; die vorgelegte Gleichung ist folglich (Lehrsatz II) lösbar.

581. Die im Vorhergehenden dargelegte Theorie liefert einen neuen Beweis der Unmöglichkeit, die allgemeinen Gleichungen über den vierten Grad hinaus algebraisch zu lösen. Im Falle der allgemeinen Gleichung fünften Grades ist nämlich die Bedingung des Lehrsatzes IV nicht erfüllt, die Gleichung folglich nicht lösbar. Die Unmöglichkeit, die allgemeine Gleichung fünften Grades zu lösen, zieht dieselbe Unmöglichkeit hinsichtlich der allgemeinen Gleichungen höherer Grade nach sich.

Untersuchungen von Hermite.

582. Es dürfte von Nutzen sein, eine mir von Hermite mitgetheilte Untersuchung hier vorzuführen, deren Zweck ist, den folgenden Satz von Galois zu beweisen:

Wenn zwei beliebige Wurzeln einer algebraisch lösbaren irreductibelen Gleichung, deren Grad eine Primzahl ist, gegeben sind, so lassen sich die übrigen daraus rational herleiten.

Hilfssatz I. — Es seien

$$F(x) = 0$$

eine irreductibele Gleichung beliebigen Grades n, und

$$x_0, x_1, x_2, \ldots, x_{n-1}$$

die n Wurzeln dieser Gleichung. Wenn alle Functionen der Wurzeln, welche durch die Substitutionen von der Form

$$x_k, x_{k+1} \text{ oder } \binom{k+1}{k}$$

(die Indices werden, wie bei Galois, in Beziehung auf den Modul n genommen) keine Aenderung erleiden, in rationaler Form bekannt sind, so kann man eine ganze Function $\varphi(x)$ vom Grade $n-1$ rational bestimmen, für welche man

$$x_1 = \varphi(x_0),\ x_2 = \varphi(x_1),\ \ldots,\ x_{k+1} = \varphi(x_k),\ \ldots,\ x_0 = \varphi(x_{n-1})$$

hat.

Es ist nämlich

$$F(x) = (x-x_0)\,(x-x_1)\,\ldots\,(x-x_{n-1}),$$

und wenn man

$$\varphi(x) = \frac{F(x)}{x-x_0}\cdot\frac{x_1}{F'(x_0)} + \frac{F(x)}{x-x_1}\cdot\frac{x_2}{F'(x_1)} + \cdots + \frac{F(x)}{x-x_{n-1}}\cdot\frac{x_0}{F'(x_{n-1})}$$

setzt, so ist $\varphi(x)$ offenbar eine ganze Function $(n-1)^{\text{ten}}$ Grades in x, deren Coefficienten Functionen der Wurzeln sind, welche durch die Substitutionen von der Form x_k, x_{k+1} keine Aenderung erleiden. Man sieht auch sofort, dass

$$\varphi(x_0) = x_1,\ \varphi(x_1) = x_2,\ \ldots$$

ist, w. z. b. w.

583. Hilfssatz II. — Es bezeichne die Primzahl n den Grad einer irreductibelen Gleichung und ϱ eine primitive Wurzel von n. Kennt man dann in rationaler Form alle Functionen der Wurzeln dieser Gleichung, welche durch die Substitutionen von den Formen x_k, x_{k+1} und x_k, $x_{\varrho k}$ keine Aenderung erleiden, so lässt sich eine ganze Function $(n-1)^{\text{ten}}$ Grades $\varphi(x)$ rational bestimmen, für welche man

$$(x_1 + \lambda x_\varrho + \lambda^2 x_{\varrho^2} + \cdots + \lambda^{n-2} x_{\varrho^{n-2}})^{n-1} = \varphi(x_0),$$

$$(x_2 + \lambda x_{\varrho+1} + \lambda^2 x_{\varrho^2+1} + \cdots + \lambda^{n-2} x_{\varrho^{n-2}+1})^{n-1} = \varphi(x_1),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots,$$

$$(x_n + \lambda x_{\varrho+n-1} + \lambda^2 x_{\varrho^2+n-1} + \cdots + \lambda^{n-2} x_{\varrho^{n-2}+n-1})^{n-1} = \varphi(x_{n-1})$$

hat; darin werden die Indices immer in Beziehung auf den Modul n genommen, und es bezeichnet λ eine Wurzel der binomischen Gleichung $\lambda^{n-1} = 1$.

Dies zu beweisen, werden wir darthun, dass das System der

linearen Gleichungen, die zwischen den unbestimmten Coefficienten der Function φ aufgestellt sind, sich nicht ändert, wenn man irgend eine Wurzel x_k durch x_{k+1}, und ebenso, wenn man x_k durch $x_{\varrho k}$ ersetzt.

Der erste Punkt ist ohne Weiteres einleuchtend; denn jede Gleichung geht aus der vorhergehenden dadurch hervor, dass man den Indices der Wurzeln eine Einheit hinzufügt, und durch dasselbe Verfahren geht die erste Gleichung aus der letzten hervor.

Der zweite Punkt lässt sich gleichfalls sehr leicht hinsichtlich der Gleichung

$$(x_1 + \lambda x_\varrho + \lambda^2 x_{\varrho^2} + \cdots + \lambda^{n-2} x_{\varrho^{n-2}})^{n-1} = \varphi(x_0)$$

bewahrheiten. Die $(n-1)^{\text{te}}$ Potenz der linearen Function

$$x_1 + \lambda x_\varrho + \lambda^2 x_{\varrho^2} + \cdots + \lambda^{n-2} x_{\varrho^{n-2}}$$

bleibt nämlich unverändert, wenn man diese Function mit λ multiplicirt. Dies läuft darauf hinaus, die Indices der Wurzeln mit ϱ zu multipliciren, wodurch das zweite Glied $\varphi(x_0)$ gleichfalls nicht verändert wird. Anders verhalten sich dagegen die übrigen Gleichungen des Systems. In irgend einer derselben

$$(x_{1+\alpha} + \lambda x_{\varrho+\alpha} + \lambda^2 x_{\varrho^2+\alpha} + \cdots + \lambda^{n-2} x_{\varrho^{n-2}+\alpha})^{n-1} = \varphi(x_\alpha)$$

machen wir $\alpha \equiv \varrho^\mu$ (*mod.* n); es ist dies möglich, weil α nicht mehr den Werth Null annimmt. Man erhält dadurch

$$(1). \quad \begin{cases} (x_{1+\varrho^\mu} + \lambda x_{\varrho+\varrho^\mu} + \lambda^2 x_{\varrho^2+\varrho^\mu} + \cdots \\ \qquad\qquad + \lambda^{n-2} x_{\varrho^{n-2}+\varrho^\mu})^{n-1} = \varphi(x_{\varrho^\mu}), \end{cases}$$

und wenn die Indices mit ϱ multiplicirt werden,

$$(2). \quad \begin{cases} (x_{\varrho+\varrho^{\mu+1}} + \lambda x_{\varrho^2+\varrho^{\mu+1}} + \lambda^2 x_{\varrho^3+\varrho^{\mu+1}} + \cdots \\ \qquad\qquad + \lambda^{n-2} x_{\varrho^{n-1}+\varrho^{\mu+1}})^{n-1} = \varphi(x_{\varrho^{\mu+1}}). \end{cases}$$

Nun ändert sich die $(n-1)^{\text{te}}$ Potenz der linearen Function

$$x_{\varrho+\varrho^{\mu+1}} + \lambda x_{\varrho^2+\varrho^{\mu+1}} + \cdots + \lambda^{n-2} x_{\varrho^{n-1}+\varrho^{\mu+1}}$$

nicht, wenn man sie mit λ multiplicirt. Man kann daher statt der Gleichung (2) die folgende schreiben:

$$(x_{\varrho^{n-1}+\varrho^{\mu+1}} + \lambda x_{\varrho+\varrho^{\mu+1}} + \lambda^2 x_{\varrho^2+\varrho^{\mu+1}} + \cdots$$
$$\qquad\qquad + \lambda^{n-2} x_{\varrho^{n-2}+\varrho^{\mu+1}})^{n-1} = \varphi(x_{\varrho^{\mu+1}}).$$

Beachtet man aber, dass $\varrho^{n-1} \equiv 1$ (*mod.* n) ist, so erkennt man,

dass die letzte Gleichung aus (1) entsteht, wenn man μ in $\mu + 1$ verwandelt.

Daraus geht hervor, dass die Substitution $x_k, x_{\varrho k}$ unsere Gleichungen nur cyclisch permutirt, wenn die Reihenfolge derselben die im Lehrsatze angegebene ist. Löst man diese Gleichungen in Beziehung auf die Coefficienten von φ auf, so gelangt man zu rationalen Functionen der Wurzeln, welche durch die Substitutionen x_k, x_{k+1} und x_k, x_{ϱ^k} keine Aenderung erleiden. Diese Coefficienten lassen sich also, wie wir behauptet hatten, rational ausdrücken. Unser Hilfssatz ist somit bewiesen; es ergiebt sich daraus der folgende Satz:

584. Hilfssatz III. — Wenn eine Gleichung, deren Grad n eine Primzahl ist, algebraisch gelöst werden kann, so gehört die durch Unterdrückung eines linearen Factors daraus gebildete Gleichung $(n-1)^{\text{ten}}$ Grades zur Klasse der Abel'schen Gleichungen.

In der That ist hinsichtlich der Gleichung $(n-1)^{\text{ten}}$ Grades, welche durch die Unterdrückung des Factors $x - x_\alpha$ entsteht, und deren Wurzeln durch

$$x_{1+\alpha}, \; x_{\varrho+\alpha}, \; x_{\varrho^2+\alpha}, \; \cdots, \; x_{\varrho^{n-2}+\alpha}$$

dargestellt werden, die resolvirende Function

$$\left(x_{1+\alpha} + \lambda x_{\varrho+\alpha} + \lambda^2 x_{\varrho^2+\alpha} + \cdots + \lambda^{n-2} x_{\varrho^{n-2}+\alpha}\right)^{n-1}$$

in rationaler Form bekannt.

585. Die drei vorstehenden Hilfssätze setzen uns in den Stand, den Lehrsatz, den wir im Auge haben, sehr leicht zu beweisen. Wir machen für einen Augenblick

$$x_{\varrho^k+\alpha} = X_k.$$

Da wir (Hilfssatz III) den Ausdruck

$$\left(X_0 + \lambda X_1 + \lambda^2 X_2 + \cdots + \lambda^{n-2} X_{n-2}\right)^{n-1}$$

als rationale Function von x_α kennen, so dürfen wir auch jede rationale Function der Wurzeln X_k als bekannt ansehen, welche durch die Substitutionen von der Form X_k, X_{k+1} keine Aenderung erleidet. Dies versetzt uns in die Bedingungen des Hilfssatzes I. Wir können also eine Function φ von der Beschaffenheit bilden, dass allgemein

$$X_{k+1} = \varphi(X_k)$$

ist. Ausserdem lassen sich die Coefficienten dieser Function rational durch die bekannten Grössen und die Wurzel x_α ausdrücken; es ist also

$$X_{k+1} = \varphi\,(X_k\,,\, x_\alpha)\,,\ \text{oder}\ x_{\varrho^{k+1}+\alpha} = \varphi\,(x_{\varrho^k+\alpha}\,,\, x_\alpha).$$

Man kann nun $\varrho^k \equiv \beta$ nehmen, wo β irgend eine von Null verschiedene ganze Zahl ist; dann folgt

$$x_{\varrho\beta+\alpha} = \varphi\,(x_{\beta+\alpha}\,,\, x_\alpha).$$

Diese Gleichung drückt genau die Relation aus, die wir zu beweisen hatten. Sie zeigt sehr leicht, wie alle Wurzeln nach und nach durch zwei beliebige Wurzeln x_α und $x_{\alpha+\beta}$ ausgedrückt werden, und lässt unmittelbar erkennen, in welcher Reihenfolge die einen aus den anderen hervorgehen.

586. Umgekehrt lässt sich leicht darthun, dass die Gleichung algebraisch gelöst werden kann, wenn die vorhergehende Relation zwischen drei Wurzeln x_α, $x_{\alpha+\beta}$, $x_{\alpha+\varrho\beta}$ besteht:

Zu diesem Zwecke sei ϑ eine Wurzel der binomischen Gleichung $x^n = 1$ und

$$F\,(\vartheta) = (x_0 + \vartheta x_1 + \vartheta^2 x_2 + \cdots + \vartheta^{n-1} x_{n-1})^n$$

die resolvirende Function von Lagrange. Diese Function hat die characteristische Eigenschaft, keine Aenderung zu erleiden, wenn man den Indices der Wurzeln eine beliebige ganze Zahl α hinzufügt. Man kann daher

$$F\,(\vartheta) = (x_\alpha + \vartheta\, x_{\alpha+1} + \vartheta^2 x_{\alpha+2} + \cdots + \vartheta^{n-1} x_{\alpha+n-1})^n$$

schreiben. Dies vorausgesetzt, sei β eine zweite willkürliche ganze Zahl, die jedoch von Null verschieden ist, und es werde β_0 so gewählt, dass man

$$\beta\beta_0 \equiv 1\ (mod.\ n)$$

hat. Dann ergiebt sich unmittelbar

$$F\,(\vartheta^{\beta_0}) = (x_\alpha + \vartheta\, x_{\alpha+\beta} + \vartheta^2 x_{\alpha+2\beta} + \cdots + \vartheta^{n-1} x_{\alpha+(n-1)\beta})^n,$$

und es ist klar, dass man durch eine Reihe von Substitutionen mittels der Relation

$$x_{\varrho\beta+\alpha} = \varphi\,(x_{\beta+\alpha}\,,\, x_\alpha)$$

das zweite Glied in eine rationale Function Π der beiden Wurzeln $x_\alpha, x_{\alpha+\beta}$ verwandeln kann, so dass für einen beliebigen Werth des willkürlichen Index α

$$F\,(\vartheta^{\beta_0}) = \Pi\,(x_\alpha\,,\, x_{\alpha+\beta})$$

ist.

Ist nun wieder λ eine Wurzel der binomischen Gleichung $x^{n-1} = 1$, so behält die Function

$$[\Pi(x_\alpha, x_{\alpha+\beta}) + \lambda\,\Pi(x_\alpha, x_{\alpha+\varrho\beta}) + \lambda^2\,\Pi(x_\alpha, x_{\alpha+\varrho^2\beta}) + \cdots + \lambda^{n-2}\,\Pi(x_\alpha, x_{\alpha+\varrho^{n-2}\beta})]^{n-1}$$

denselben Werth, wenn man $\varrho\beta$ an die Stelle von β setzt, d. h. sie ist von dem β ertheilten Werthe unabhängig. Ausserdem ist jeder ihrer Terme von α unabhängig. Wird diese Function also mittels der Relation

$$x_{\alpha+\varrho\beta} = \varphi(x_{\alpha+\beta}, x_\alpha)$$

in eine rationale Function der beiden Wurzeln x_α, $x_{\alpha+\beta}$ transformirt, so muss sie sich auf eine bekannte Grösse reduciren. Wenn nämlich eine Function

$$u = \psi(x_{\alpha+\beta}, x_\alpha)$$

für alle Werthe der Indices α, β, von denen der letzte von Null verschieden ist, denselben Werth behält, so kann man

$$n(n-1)\,u = \sum_{\alpha=0}^{\alpha=n-1} \sum_{\beta=1}^{\beta=n-1} \psi(x_{\alpha+\beta}, x_\alpha)$$

schreiben, und das zweite Glied dieser Relation ist eine symmetrische Function aller Wurzeln $x_0, x_1, \ldots, x_{n-1}$.

Daraus ergiebt sich, dass die $n-1$ Grössen

$$\Pi(x_\alpha, x_{\alpha+\beta}),\ \Pi(x_\alpha, x_{\alpha+\varrho\beta}),\ \ldots,\ \Pi(x_\alpha, x_{\alpha+\varrho^{n-2}\beta})$$

als die Wurzeln einer durch die Ausziehung einer einzigen Wurzel $(n-1)^{\text{ten}}$ Grades auflösbaren Abel'schen Gleichung angesehen werden können. Hat man diese Grössen einmal bestimmt, so kennt man die n^{te} Potenz der resolvirenden Function $F(\vartheta^{\beta_0})$ für alle Werthe von β, den Werth $\beta = 0$ ausgenommen. Durch Ausziehung von $n-1$ Wurzeln n^{ten} Grades erhalten wir also diese verschiedenen resolvirenden Functionen, und folglich die Wurzeln selbst. Ausserdem weiss man nach einer Bemerkung von Abel, dass man diese $n-1$ Wurzeln durch rationale Functionen einer derselben und der Grössen, auf die sie sich beziehen, ausdrücken kann; die letzteren Grössen sind, wie schon gesagt, die Wurzeln einer Abel'schen Gleichung.

Untersuchungen von Kronecker.

587. Zum Schluss dieses Werkes wollen wir eine Arbeit von Kronecker wörtlich folgen lassen, welche Lejeune-

Dirichlet der Berliner Akademie der Wissenschaften am 20. Juni 1853 vorlegte.

„Die bisherigen Untersuchungen über die Auflösbarkeit von Gleichungen, deren Grad eine Primzahl ist — namentlich die Abel'schen und Galois'schen, welche die Grundlage aller weiteren Forschungen in diesem Gebiete bilden — haben im Wesentlichen als Resultat zwei Kriterien ergeben, vermittelst deren man beurtheilen könnte, ob eine gegebene Gleichung auflösbar sei oder nicht. Indessen gaben diese Kriterien über die Natur der auflösbaren Gleichungen selbst eigentlich nicht das geringste Licht. Ja man konnte eigentlich gar nicht wissen, ob (ausser den von Abel im IV^ten Bande des Crelle'schen Journals behandelten und den einfachsten mit den binomischen Gleichungen zusammenhängenden) überhaupt noch irgend welche Gleichungen existiren, welche die gegebenen Auflösbarkeits-Bedingungen erfüllen. Noch weniger konnte man solche Gleichungen bilden, und man ist auch durch sonstige mathematische Untersuchungen nirgends auf solche Gleichungen geführt worden. Dazu kommt noch, dass jene beiden erwähnten und wohl allgemein bekannten, von Abel und Galois gegebenen Eigenschaften der auflösbaren Gleichungen zufälliger Weise solche waren, die die wahre Natur dieser Gleichungen eher zu verdecken, als aufzuklären geeignet sein dürften, wie ich das namentlich von dem einen jener beiden Kriterien späterhin zeigen werde. Und so blieben die auflösbaren Gleichungen selbst in einem gewissen Dunkel, welches nur durch die übrigens, wie es scheint, wenig beachtete und ganz specielle Notiz Abel's über die Wurzeln ganzzahliger Gleichungen fünften Grades ein wenig erhellt wurde, und welches nur durch die Auflösung des Problems: „Alle auflösbaren Gleichungen zu finden“ vollständig aufgeklärt werden konnte. Denn alsdann hat man nicht blos unendlich viele neue auflösbare Gleichungen, sondern eben alle möglichen gewissermassen vor Augen und kann an der entwickelten Form ihrer Wurzeln alle ihre Eigenschaften auffinden und erweisen.

„Diesen wenigen Bemerkungen über den Zielpunkt meiner Untersuchungen und den wesentlichen Inhalt der vorliegenden Notizen habe ich nur hinzuzufügen, dass das eben erwähnte Problem, welches ich mir von vornherein gestellt hatte, freilich noch gänzlich umzuformen war, um es für eine Untersuchung

34*

geeignet zu machen. Die genaue Formulirung des Problems selbst ist aber hier von so grosser Wichtigkeit, dass ich in den folgenden Mittheilungen gerade in dieser Hinsicht etwas weitläufiger sein muss, um nicht durch die Kürze der Klarheit Abbruch zu thun.

„Abel hat in seiner fragmentarischen Abhandlung über die algebraische Auflösung der Gleichungen (No. XV des II. Bandes der gesammelten Werke) unter anderen Problemen wörtlich folgendes aufgestellt: „Den allgemeinsten algebraischen Ausdruck zu finden, welcher einer Gleichung von einem gegebenen Grade genügen könne.“ Fügt man diesem Problem Dasjenige hinzu, welches erforderlich ist, um es zu einem bestimmten zu machen, so enthält es in der That alle Probleme in sich, die man in Bezug auf die Auflösbarkeit der Gleichungen stellen kann, und ist namentlich die wichtigste Verallgemeinerung des (als in gewissem Sinne zu speciellen) unlösbaren Problems: „Die Wurzel einer Gleichung irgend eines Grades als algebraische Function ihrer Coefficienten auszudrücken.“ Es ist nun aber, wie gesagt, bei obigem Probleme noch erforderlich, den Zusammenhang zwischen dem gesuchten algebraischen Ausdrucke und den Coefficienten der Gleichung zu bestimmen; deshalb ist die Aufgabe vielmehr dahin zu stellen:

„Die allgemeinste algebraische Function irgend welcher Grössen $A, B, C,$ u.s.w. zu finden, welche einer Gleichung von einem gegebenen Grade genügt, deren Coefficienten rationale Functionen jener Grössen sind.

„Es ist hierbei zu bemerken, dass man die Irreductibilität der Gleichung in Bezug auf A, B, C u. s. w. vorauszusetzen hat; d. h. die Gleichung soll (so lange man für $A, B, C,$ u. s. w. nicht irgend welche specielle Werthe substituirt) nicht in Factoren niederen Grades zerlegt werden können, deren Coefficienten wiederum rationale Functionen von $A, B, C,$ u. s. w. sind. Das obige Problem kann danach auch folgendermassen ausgedrückt werden:

„Für eine gegebene Zahl n die allgemeinste algebraische Function von $A, B, C,$ u. s. w. zu finden, welche durch die Variirung der darin enthaltenen Wurzelzeichen verschiedene Ausdrücke ergiebt, unter denen

n so beschaffen sind, dass ihre symmetrischen Functionen sämmtlich rationale Functionen jener Grössen A, B, C, u. s. w. sind.

„Für den Fall nun, dass der gegebene Grad der Gleichung resp., nach der zweiten Ausdrucksweise, die Anzahl der Werthe eine Primzahl ist, hat Abel die Untersuchung in der angeführten Abhandlung im Wesentlichen so weit geführt, dass er die folgenden beiden Formen angab, welche die gesuchten algebraischen Functionen haben müssen:

$$(1). \qquad p_0 + s^{\frac{1}{\mu}} + f_2(s) \cdot s^{\frac{2}{\mu}} + \cdots + f_{\mu-1}(s) \cdot s^{\frac{\mu-1}{\mu}}$$

(pag. 204 des II. Bandes der gesammelten Werke), wo unter der Primzahl μ der gegebene Grad der Gleichung, unter p_0 eine rationale Function, unter s eine algebraische Function von A, B, C, u. s. w. und unter $f_k(s)$ eine rationale Function von s und von A, B, C, u. s. w. zu verstehen ist. — Die zweite Form findet sich pag. 190 desselben Bandes und Werkes und ist:

$$(2). \qquad p_0 + R_1^{\frac{1}{\mu}} + R_2^{\frac{1}{\mu}} + \cdots + R_{\mu-1}^{\frac{1}{\mu}},$$

wo p_0 eine rationale Function von A, B, C, u. s. w. ist, und $R_1, R_2, \ldots$ Wurzeln einer Gleichung $(\mu - 1)^{\text{ten}}$ Grades bedeuten, deren Coefficienten rationale Functionen von A, B, C, u. s. w. sind. — Für diese beiden Formen hat Malmsten einen ausführlichen Beweis im 34. Bande des Crelle'schen Journals gegeben, der jedoch, wie ich glaube, einige Vervollständigungen noch wünschenswerth erscheinen lässt.

„Jene beiden Formen muss nun zwar nothwendig jede algebraische Function haben, wenn sie dem Probleme Genüge leisten soll; aber die Formen sind noch zu allgemein, d. h. sie schliessen noch solche algebraische Functionen in sich, die dem Probleme nicht Genüge leisten. Ich habe deshalb jene beiden Formen näher untersucht und zuvörderst gefunden, dass diejenigen in der Form (2) enthaltenen algebraischen Functionen, welche dem Probleme genügen, die Eigenschaft haben müssen, dass nicht nur (wie Abel bemerkt hat) die symmetrischen Functionen der Grössen $R_1, R_2, \ldots$, sondern auch — wenn man diese in einer gewissen Ordnung nimmt — die cyclischen Functionen*)

*) Unter einer cyclischen Function von $x_1, x_2, \ldots, x_n$ versteht

derselben rationale Functionen der A, B, C, u. s. w. sein müssen, d. h. dass die Gleichung $(\mu - 1)^{\text{ten}}$ Grades, deren Wurzeln die Grössen R_1, R_2, ... sind, eine Abel'sche ist. Ich verstehe hier unter Abel'schen Gleichungen immer jene besondere Klasse auflösbarer Gleichungen, welche Abel in dem mémoire XI des ersten Bandes der gesammelten Werke behandelt hat, und welche (wenn man annimmt, dass ihre Coefficienten rationale Functionen von A, B, C, u. s. w. und ihre Wurzeln nach einer bestimmten Ordnung genommen x_1, x_2, ..., x_n sind) ebensowohl dadurch definirt werden können, dass die cyclischen Functionen der Wurzeln rationale Functionen von A, B, C, u. s. w. sind, als dadurch, dass die Gleichungen

$$x_2 = \vartheta(x_1),\ x_3 = \vartheta(x_2),\ \ldots,\ x_n = \vartheta(x_{n-1}),\ x_1 = \vartheta(x_n)$$

statt haben, wo $\vartheta(x)$ eine ganze rationale Function von x bedeutet, deren Coefficienten rationale Functionen von A, B, C, u. s. w. sind. Auf diese besondere Klasse von Gleichungen, die übrigens von dem grössten Interesse für die Analysis und Zahlentheorie und, wie man hier sieht, auch für die Algebra selbst ist, werde ich unten noch zurückkommen.

„Eine weitere Untersuchung der obigen Formen (1) und (2) ergiebt aber noch folgende nähere Bestimmung für diejenigen Grössen R, welche die Form (2) zu einer dem Probleme genügenden machen. Es muss nämlich

$$(3).\qquad R_k = F(r_k)^{\mu} \cdot r_k^{\gamma-1} \cdot r_{k+1}^{\gamma-2} \cdot r_{k+2}^{\gamma-3} \cdots r_{k+\mu-2}$$

sein, wo r_k, r_{k+1}, ... die $\mu - 1$ Wurzeln irgend einer Abel'schen Gleichung $(\mu - 1)^{\text{ten}}$ Grades sind, d. h. wo sowohl die symmetrischen als die cyclischen Functionen der Grössen r (die Anordnung derselben nach den Indices genommen) rationale Functionen von A, B, C, u. s. w. sind; wo ferner $F(r)$ irgend eine rationale Function von r und von A, B, C, u. s. w., und wo endlich γ_m den kleinsten positiven Rest von g^m *mod.* μ bedeutet, wenn g eine primitive Wurzel von μ ist. Substituirt man diesen Ausdruck von R_k in (2), so erhält man eine Form, welche nicht nur jeder dem Probleme genügende Ausdruck haben muss, sondern welche auch (und das ist die Hauptsache) nur solche Ausdrücke

---

man den Ausdruck $(x_1 + \alpha x_2 + \alpha^2 x_3 + \cdots + \alpha^{n-1} x_n)^n$, in welchem α eine Wurzel von $\alpha^n = 1$ ist.

enthält, die dem Probleme genügen; d. h. die so entstandene Form erfüllt als Wurzel identisch eine Gleichung μ^{ten} Grades, deren Coefficienten rationale Functionen von A, B, C, u. s. w. sind. Die übrigen Wurzeln werden durch Aenderung des μ^{ten} Wurzelzeichens in (2) erhalten, und zwar in der Weise, dass die m^{te} Wurzel z_m durch folgende Gleichung bestimmt wird:

$$(4).\quad z_m = p_0 + \omega^m . R_1^{\frac{1}{\mu}} + \omega^{gm} . R_2^{\frac{1}{\mu}} + \omega^{g^2 m} . R_3^{\frac{1}{\mu}} + \cdots + \omega^{g^{\mu-2} m} . R_{\mu-1}^{\frac{1}{\mu}},$$

wo für die Grössen R die Ausdrücke aus (3) zu nehmen sind und ω eine imaginäre μ^{te} Wurzel der Einheit bedeutet.

„Hieraus geht zuvörderst hervor, dass, während die symmetrischen Functionen der Grössen z eben rationale Functionen von A, B, C, u. s. w. sind, die cyclischen Functionen derselben (wenn man die Ordnung nach den Indices nimmt) rationale Functionen von A, B, C, u. s. w. und von $r_1, r_2, \ldots$ und von ω sind. Da aber die Grössen r selbst Wurzeln einer Abel'schen Gleichung und also $r_2, r_3, \ldots$ rationale Functionen von r_1 und A, B, C, u. s. w. sind, so heisst dies nichts Anderes, als: Jede auflösbare Gleichung von einem Primzahlgrade μ ist eine Abel'sche, wenn man eine Grösse ϱ_1 als bekannt annimmt, welche selbst Wurzel einer Abel'schen Gleichung $(\mu - 1)^{ten}$ Grades ist; oder auch: Die μ Wurzeln einer auflösbaren Gleichung sind immer dergestalt unter einander verbunden, dass

$$z_2 = f(z_1, \varrho_1), \; z_3 = f(z_2, \varrho_1), \ldots, z_1 = f(z_\mu, \varrho_1),$$

wo $f(z, \varrho_1)$ eine rationale Function von z, von ϱ_1 und von A, B, C, u. s. w. bedeutet, und ϱ_1 die Wurzel einer Abel'schen Gleichung ist, deren Coefficienten rationale Functionen von A, B, C, u. s. w. sind*). Diese Relation zwischen den Wurzeln einer jeden auflösbaren Gleichung ist übrigens die wahre Quelle jener von Abel und

*) Es sind hier einige von Kronecker selbst angegebene Berichtigungen gemacht. Die durch ϱ_1 dargestellte Grösse ist in den Jahresberichten der Berliner Akademie mit r_1 bezeichnet. Diese neue Wurzel ϱ_1 steht zwar in einem sehr einfachen Zusammenhange mit r_1; beide Grössen sind jedoch von einander verschieden.

Galois als charakteristisches Merkmal der Wurzeln auflösbarer Gleichungen von Primzahlgraden angegebenen Eigenschaft, dass eine Wurzel rationale Function zweier anderen sein müsse. Im Uebrigen hebe ich unter vielen interessanten Folgerungen, die man aus den gegebenen Resultaten ziehen kann, nur noch die eine hervor, dass, da r_1 als Wurzel einer Abel'schen Gleichung $(\mu - 1)^{\text{ten}}$ Grades nur solche Wurzelzeichen als nothwendige enthalten kann, deren Exponenten Theiler von $\mu - 1$ sind, auch nur eben solche Wurzelzeichen und μ^{te} Wurzelzeichen selbst in der Wurzel jeder auflösbaren Gleichung als nothwendige vorkommen. Abel hat die betreffende Bemerkung (soweit mir bekannt ist) nur für $\mu = 5$ gemacht und für diesen Fall auch die allgemeinste Wurzelform einer auflösbaren Gleichung gegeben (Band II, p. 253 der gesammelten Werke). Er hat aber dabei — was wohl zu bemerken ist — die Beschränkung hinzugefügt, dass die Coefficienten der Gleichung rationale Zahlen sein sollen.

„Das Hauptproblem ist nun durch die Gleichung (3) darauf zurückgeführt, dass man die allgemeinste Form einer Grösse, oder, besser gesagt, eines Ausdrucks r_1 zu suchen hat. Dieses zweite Problem stellt sich daher nach den oben über $r_1, r_2, \ldots$ gemachten Bestimmungen also:

„Für eine bestimmte Zahl n die allgemeinste Form einer algebraischen Function von A, B, C, u. s. w. zu finden, welche durch die Variirung der darin enthaltenen Wurzelzeichen verschiedene Ausdrücke ergiebt, unter denen n so beschaffen sind, dass deren symmetrische und cyclische Functionen (wenn man eine bestimmte Ordnung fixirt) rationale Functionen von A, B, C, u. s. w. sind.

„Und so bedeutet dieses zweite Problem, so zu sagen, roh ausgedrückt, nichts anderes als alle Abel'schen Gleichungen zu finden, ebenso wie das Hauptproblem gewissermassen alle auflösbaren Gleichungen finden hiess.

„In Beziehung auf dieses zweite Problem wird man nun ebenfalls wieder auf eine Unterscheidung geführt, je nachdem n Primzahl, Primzahlpotenz oder allgemein zusammengesetzte Zahl ist; und zwar wird das Problem für ein allgemeines n dadurch

erledigt, dass man dasselbe nur für alle diejenigen Fälle zu lösen hat, wo der Grad der Abel'schen Gleichung eine der in n enthaltenen Primzahlpotenzen ist. In diesen Fällen aber bietet das Problem, mit Ausnahme einiger blossen Complicationen, auch keine grössere Schwierigkeit dar, als wenn n eine Primzahl selbst ist. Nur in dem anscheinend einfachsten Falle, wo n die dritte oder eine höhere Potenz von 2 ist, reicht die Methode, die ich in allen anderen Fällen mit Erfolg angewendet habe, zur vollständigen Lösung des Problems nicht aus, und ich habe die alsdann erforderliche Modification derselben noch nicht ergründet. Da nun die vollständige Lösung des Hauptproblems für eine Primzahl μ die Lösung des zweiten Problems für $n = \mu - 1$ erfordert, so würde ich immerhin für jetzt das vollständige Resultat nur für diejenigen Primzahlen μ, welche nicht von der Form $8h + 1$ sind, angeben können. Es dürfte aber ohnehin für den Zweck dieser vorläufigen Mittheilung genügen, wenn ich zur leichteren Uebersicht der Sache hier nur denjenigen Fall des zweiten Problems erörtere, wo n eine ungerade Primzahl ist. Und zwar will ich für diesen Fall nicht blos das Resultat selbst, sondern auch die bei Erlangung desselben angewendete Methode kurz angeben, zumal dieselbe ungemein einfach ist und das wesentliche Mittel zur Auflösung dieses zweiten Problems in allen anderen Fällen und auch des Hauptproblems selbst bildet.

„Wenn man sich der von Abel (in der oben angeführten Abhandlung No. XI des I. Bandes der gesammelten Werke) angewendeten Ausdrucksweise bedient, so kann man mit Rücksicht auf die oben gegebenen Definitionen der Abel'schen Gleichungen das in Rede stehende Problem folgendermassen ausdrücken:

„Die allgemeinste algebraische Function von A, B, C, u. s. w. zu finden, welche einer Gleichung n^{ten} Grades genügt, deren Coefficienten rationale Functionen von A, B, C, u. s. w. sind, und deren übrige Wurzeln (wenn man dieselben mit $z_1, z_2, \ldots, z_{n-1}$ und die gesuchte Function selbst mit z_0 bezeichnet) die Gleichungen erfüllen:

$$z_1 = \vartheta(z_0),\ z_2 = \vartheta(z_1),\ \ldots,\ z_0 = \vartheta(z_{n-1}),$$

wo $\vartheta(z)$ eine rationale Function von z und von A, B, C, u. s. w. bedeutet.

„Setzt man nun, unter der Annahme, dass n Primzahl, nach

der von Jacobi bei der Kreistheilung eingeführten Bezeichnung den Ausdruck

$$z_0 + z_1 \alpha + z_2 \alpha^2 + \ldots + z^{n-1} \alpha^{n-1} = (\alpha\,,\, z),$$

wo α eine n^{te} Wurzel der Einheit bedeutet, so ist

$$(5).\ n z_k = (1, z) + \alpha^{-k}(\alpha\,,\, z) + \alpha^{-2k}(\alpha^2\,,\, z) + \cdots + \alpha^{-(n-1)k}(\alpha^{n-1}, z).$$

Man kann ferner nach der von Abel angegebenen Weise zeigen, dass für jede beliebige ganze Zahl k die Gleichungen statthaben:

$$(6).\quad \left\{ \begin{array}{l} (\alpha\,,\, z)^k = (\alpha^k\,,\, z)\ \varphi(\alpha)\,,\ (\alpha^2\,,\, z)^k = (\alpha^{2k}\,,\, z)\ \varphi(\alpha^2), \\ \qquad (\alpha^3\,,\, z)^k = (\alpha^{3k}\,,\, z)\ \varphi(\alpha^3)\,, \ldots, \end{array} \right.$$

wo $\varphi(\alpha)$ eine rationale Function von α und von $A, B, C,$ u. s. w. bedeutet.

„Wenn man nun für k eine primitive Wurzel g der Primzahl n und zwar eine solche setzt, für die $g^{n-1} - 1$ durch keine höhere Potenz von n als durch n selbst theilbar ist, so wird man Gleichungen von folgender Form erhalten:

$$(\alpha\,,\, z)^g = (\alpha^g\,,\, z)\ f(\alpha)\,,\ (\alpha^g\,,\, z)^g = (\alpha^{g^2}\,,\, z)\ f(\alpha^g)\,, \ldots,$$
$$(\alpha^{g^{n-2}}\,,\, z)^g = (\alpha\,,\, z)\ f(\alpha^{g^{n-2}}).$$

Erhebt man von diesen Gleichungen die erste zur Potenz g^{n-2}, die zweite zur Potenz g^{n-3}, u. s. f., und multiplicirt sie alsdann sämmtlich mit einander, so erhält man

$$(7).\quad (\alpha\,,\, z)^{g^{n-1}-1} = f(\alpha)^{g^{n-2}} \cdot f(\alpha^g)^{g^{n-3}} \ldots f(\alpha^{g^{n-2}}).$$

Setzt man nun

$$g^{n-1} - 1 = m \,.\, n,$$

wo m nach der in Bezug auf g gemachten Voraussetzung nicht durch n theilbar ist, so hat man mit Hilfe der Gleichung (6)

$$(\alpha\,,\, z)^{g^{n-1}-1} = (\alpha\,,\, z)^{mn} = (\alpha^m\,,\, z)^n\ \varphi(\alpha)^n\,,$$

und dies in (7) eingesetzt

$$(\alpha^m\,,\, z)^n\ \varphi(\alpha)^n = f(\alpha)^{g^{n-2}} \cdot f(\alpha^g)^{g^{n-3}} \ldots f(\alpha^{g^{n-2}}),$$

ein Resultat, welches, wie man genau zeigen kann, für jedes α richtig bleibt, und welches leicht in folgende Form umgewandelt wird:

$$(8).\ (\alpha^m, z) = F(\alpha^m) \left\{ f(\alpha^m) \cdot f(\alpha^{2m})^{\frac{1}{2}} \cdot f(\alpha^{3m})^{\frac{1}{3}} \ldots f(\alpha^{(n-1)m})^{\frac{1}{n-1}} \right\}^{\frac{1}{n}},$$

wo unter den gebrochenen Exponenten innerhalb der Parenthese nicht diese selbst, sondern die kleinsten positiven Reste dieser Brüche *mod.* n zu verstehen sind, und wo $f(\alpha)$ sowohl als $F(\alpha)$ rationale Functionen von α und von A, B, C, u. s. w. bedeuten. Setzt man diesen Ausdruck für (α^m, z) in der Gleichung (5) ein, so erhält man eine Form, die z_k haben muss, die aber auch in allen Fällen (d. h. wenn man für $f(\alpha)$ und $F(\alpha)$ irgend welche rationale Functionen von α und A, B, C, u. s. w. setzt) in der That dem Probleme genügt.

„Auch aus diesem Resultate lassen sich namentlich im Vergleich mit der oben gegebenen allgemeinsten Form der Wurzel einer auflösbaren Gleichung μ^{ten} Grades interessante Folgerungen herleiten; das bei weitem grösste Interesse aber gewährt die Vergleichung des Ausdrucks (8) (unter der Annahme, dass A, B, C, u. s. w. ganze Zahlen seien) mit seinem entsprechenden Ausdrucke für gewisse specielle in der Theorie der Kreistheilung vorkommende Abel'sche Gleichungen, namentlich mit der überaus wichtigen, von Kummer (in Crelle's Journ., Bd. 35, p. 363) gegebenen Form für (α, x). Diese Vergleichung ergiebt nämlich das bemerkenswerthe und nicht bloss für den Fall eines Primzahlgrades, sondern ganz allgemein geltende Resultat:

dass die Wurzel jeder Abel'schen Gleichung mit ganzzahligen Coefficienten als rationale Function von Wurzeln der Einheit dargestellt werden kann,

so dass diese allgemeinen Abel'schen Gleichungen im Wesentlichen nichts Anderes sind, als die Kreistheilungs-Gleichungen.

„Auch zwischen den Wurzeln derjenigen Abel'schen Gleichungen, deren Coefficienten nur ganze complexe Zahlen von der Form $a + b\sqrt{-1}$ enthalten, und den Wurzeln derjenigen Gleichungen, welche bei der Theilung der Lemniscate auftreten, existirt eine ähnliche Relation, und man kann das obige Resultat endlich noch weiter für die Abel'schen Gleichungen verallgemeinern, deren Coefficienten bestimmte algebraische Zahlenirrationalitäten enthalten.

„Ich will noch bemerken, dass die Anwendung des obigen Satzes über die Wurzeln ganzzahliger Abel'schen Gleichungen auf die oben unter (3) angegebene Form ergiebt, dass die Wurzel einer jeden auflösbaren Gleichung vom μ^{ten} Grade mit ganz-

zahligen Coefficienten als eine Summe von μ^{ten} Wurzeln aus rationalen (aus Wurzeln der Einheit gebildeten) complexen Zahlen dargestellt werden kann; und es lässt sich sogar mit Hilfe solcher complexen Zahlen die allgemeinste nothwendige und hinreichende Form jeder Wurzel einer ganzzahligen auflösbaren Gleichung μ^{ten} Grades recht einfach darstellen, jedoch würden die zur genauen Angabe dieser Form erforderlichen zahlentheoretischen Vorbemerkungen die Grenzen dieser Mittheilung überschreiten.

Druckfehler.

Bd. I. p. 314. Z. 4 von oben: $f'(x)$ hat statt -1 das Zeichen $+$.
Bd. II. p. 436. Z. 14 von unten lies: „der No. 531“ statt „der vorhergehenden Nummer.“
„ „ p. 436. Z. 18 von unten lies: $+10x^3$ statt $-10x^3$.







